

María Cristina González Bedmar

**EL VALOR DE LA PRUEBA ELECTRÓNICA EN EL PROCESO PENAL
ESPAÑOL**

TRABAJO DE FIN DE GRADO

Dirigido por el Dr. Federic Adan Domenech

Grado de Derecho



UNIVERSITAT ROVIRA I VIRGILI

Tarragona

2015

ÍNDICE

1. INTRODUCCIÓN	5
2. LA PRUEBA EN EL PROCESO PENAL	7
2.1. La probática como ciencia.....	7
2.1. Las funciones de la prueba: fijar hechos, convencer al juez, la certeza	7
2.1. El derecho a la prueba como exigencia jurídica de racionalidad.....	8
3. LA PRUEBA ELECTRÓNICA: LOS NUEVOS SISTEMAS DE COMUNICACIÓN ESPECIAL	11
3.1. Régimen normativo de la prueba electrónica	11
3.1.1 La LECrim y su vinculación con la LEC 1/2000.	11
3.1.2. Normas sustantivas en relación con la prueba electrónica	12
A) Normativa internacional	12
B) Normativa comunitaria	13
C) Normativa estatal	14
3.2. La necesaria adecuación de la legislación procesal a una nueva era.....	15
3.2.1. Las tecnologías de la Información y de las Comunicaciones (TIC)	16
3.2.2. La relevancia probatoria de los soportes informáticos	17
3.3. Tratamiento doctrinal de la prueba electrónica	18
3.3.1. Concepto.....	18
3.3.2. Valor probatorio	20
3.3.2.1. La garantía de la autenticidad e integridad de la prueba.....	20
3.3.2.2. El juicio de licitud. El respecto a los derechos fundamentales	21
A) El derecho a la intimidad personal (art. 18.1CE).....	22
B) El derecho al secreto de las comunicaciones (art. 18.3CE)	22

C) El derecho a la inviolabilidad domiciliaria (art. 18.2CE)	22
3.4. Clases de prueba electrónica	22
A) Correo electrónico	22
B) Mensaje de teléfono (SMS y WHATSAPP).....	24
C) Página web.....	26
D) Registro fonográfico, videgrabación, fotografía digital	26
E) Dispositivos electrónicos de almacenamiento	27
F) Documentos electrónicos	27
4. INCORPORACIÓN DE LA PRUEBA DIGITAL EN EL PROCESO	29
4.1. Formas de acceso.....	29
4.2. En fase de instrucción.....	30
4.1.1 Aportación de la prueba electrónica por las partes	30
4.1.2. Aprehensión de dispositivo fuera de lugar cerrado	31
4.1.3 Diligencia de entrada y registro en lugar cerrado	32
4.1.4. Registros de información accesible y registro remotos	35
4.3. Durante el juicio oral.....	38
4.3.1. Procedimiento probatorio	38
4.3.2. El juicio oral	38
4.3.2.1. Como prueba pericial.....	39
4.3.2.2. Como prueba testifical.....	41
4.3.2.3. Como reconocimiento judicial.....	42
4.3.2.3. Como prueba documental	44
4.3.2.4. Como reproducción de palabras, sonidos e imágenes	45

5. EFICACIA PROBATORIA DE LA PRUEBA ELECTRÓNICA	47
5.1. La valoración de la prueba electrónica	47
5.1.1. Prueba legal, prueba libre y sistemas mixtos de valoración	48
5.1.2. Las reglas de la sana crítica, las máximas de experiencia y la certidumbre razonable.....	50
5.1.3. La exigencia jurídica de motivación.....	53
5.1.3.1. Exclusión de la prueba ilícita.....	53
5.1.3.2. Denegación motivada	54
5.1.3.3. Prohibición de toda indefensión	55
5.2. Criterios y especialidades valorativas aplicables a la prueba electrónica.....	55
5.2.1. Racionalidad	56
5.2.2. Excepción a la libre valoración.....	57
5.2.3. Acceso a la prueba electrónica.....	58
5.2.4. Manipulación	59
5.2.5. Concurrencia de pruebas.....	59
5.2.6. Pericia informática.....	60
6. LOS PROBLEMAS QUE REPRESENTA LA INFORMACIÓN DIGITAL.....	61
6.1. Proliferación y fragmentación legal	61
6.2. Los problemas procesales vinculados a la cadena de custodia.....	62
6.3. Especial relevancia en el orden penal: los delitos informáticos	64
6.3.1. Delitos informáticos a nivel europeo.....	64
6.3.2. Delitos informáticos en España	65
7. CONCLUSIONES	69
8. BIBLIOGRAFIA	73
9. ANEXO DE JURISPRUDENCIA.....	77

1. INTRODUCCIÓN

La nueva sociedad de la información conlleva grandes cambios en numerosos ámbitos y niveles de la vida, incluyendo cambios también en el mundo del Derecho.

Este progreso ha comportado una modernización en el proceso judicial, el cual ha ido incorporando paulatinamente nuevos elementos electrónicos surgidos gracias al continuo desarrollo de la tecnología y la informática.

La denominada prueba electrónica es una de las manifestaciones de tal modernización. Este tipo de prueba permite, a través de la aplicación de las nuevas tecnologías, probar hechos relevantes para el proceso mediante soportes electrónicos.

Este trabajo pretende mostrar la forma en la que se ha introducido en el proceso penal español las nuevas tecnologías como fuente de prueba. Se trata de un estudio sobre las ventajas que ofrecen y las dificultades que se observan respecto a su incorporación en el proceso así como respecto a su valoración y eficacia.

Para ello, se analiza de manera ordenada los preceptos legales reguladores de la materia, los cuales abarcan desde normativa muy específica que se ciñe a supuestos concretos, como son leyes reguladoras de un tipo específico de prueba electrónica, normativa menos específica como convenios europeos y legislación de derecho comparado.

También se estudian los criterios seguidos por distintos autores expertos en la temática, para la interpretación de los textos legales, así como los razonamientos y motivos expuestos por la jurisprudencia, en especial las resoluciones judiciales del Tribunal Supremo y del Tribunal Constitucional, atendiendo a la casuística que el tema requiere.

2. LA PRUEBA EN EL PROCESO PENAL

2.1. La probática como ciencia.

La probática es una teoría del conocimiento que se ocupa de estudiar las circunstancias históricas, psicológicas y sociológicas que llevan a la obtención del conocimiento de hechos ocurridos¹.

Pretende lograr la reconstrucción de los hechos en el proceso judicial al objeto de poder sentar su evidencia, partiendo de una previa actividad investigadora.

Su relación con el derecho procesal, y en particular con el derecho probatorio es instrumental ya que éste facilita o limita los medios para que la probática pueda cumplir su objetivo².

2.2. Las funciones de la prueba: fijar hechos, convencer al juez, la certeza.

Dentro del proceso judicial la prueba desempeña diversas funciones, las cuales pueden sintetizarse de la siguiente forma:

Fijar hechos. La ley regula una serie de mecanismos que el juzgador tiene que utilizar como sistemas para llegar a la determinación de los hechos y esa fijación es la función de las normas probatorias. Sujetar la actividad probatoria a métodos jurídicos es la mejor manera de lograr establecer los hechos en el proceso, pretendiendo lograr la seguridad en la determinación de los hechos con economía en el esfuerzo. Los hechos que no constituyen objeto de prueba o son hechos admitidos, notorios o imposibles.

Convencer al juez. La prueba busca convencer al juez. Las meras afirmaciones de las partes carecen de plena eficacia en el proceso si no se encuentran sustentadas con medios de prueba que las corroboren, y que permitirán al Juez llegar a la convicción necesaria sobre la fundabilidad o no de las pretensiones propuestas por las partes³.

¹ Definición extraída de las nociones sobre probática expuestas por Rivera Morales, Rodrigo. (2011). En “La prueba: un análisis racional y práctico”. Madrid: ed. Marcial Pons. Pág. 27. Y de lo expuesto por Muñoz Sabaté, Lluís. (2007). En la “Introducción a la probática”. Colección de Formación Continua Facultad de Derecho ESADE. Barcelona: ed. Bosch Formación. Pág. 11-15.

² Muñoz Sabaté, Lluís. (2009). *Curso de probática judicial*. Madrid: ed. La Ley. Pág. 21-25.

³ López Simó, Francisco. (2001). *Disposiciones generales sobre la prueba*. Madrid: ed. La Ley. Pág. 38 y ss.

La certeza. Si se logran probar los hechos se consigue llegar a una certeza sobre los mismos, de manera que pasan a ser ciertos los hechos que eran meramente afirmados en el momento inicial del proceso permitiendo que el juzgador llegue a la convicción de cuál es la verdad procesal en un litigio determinado⁴.

2.3. El derecho a la prueba como exigencia jurídica de racionalidad.

El derecho a la prueba está recogido en el art. 24.1 de la CE como un derecho fundamental típicamente individual, inherente a la persona, de aplicación directa, inmediata e irrenunciable, objeto de las mayores garantías⁵. Se trata del derecho que tienen las partes de convencer al juez mediante todas las pruebas que tengan a su disposición⁶.

En primer lugar, debemos hablar del derecho a utilizar todas las pruebas de que se dispone para demostrar la verdad de los hechos que fundan la pretensión.

Se trata de la capacidad jurídica que se reconoce a quien interviene como litigante en un proceso de provocar la actividad procesal necesaria para lograr la convicción del órgano judicial sobre la existencia o inexistencia de los hechos relevantes para la decisión del conflicto objeto del proceso⁷.

En segundo lugar, el derecho a la prueba incluye el derecho a que las pruebas sean practicadas en el proceso. Ello significa que una vez propuestas y admitidas, las pruebas deben ser practicadas, puesto que la ausencia de práctica de una prueba admitida equivale a una inadmisión no motivada.

De acuerdo con la jurisprudencia, la prueba por soportes electrónicos debe ser admitida y practicada siempre que se haya obtenido lícitamente el soporte, se proponga de acuerdo con lo dispuesto en la ley, sea pertinente en relación al tema de prueba y se revele como útil⁸.

En tercer lugar, dentro del art. 24.1 CE se encuadra el derecho a una valoración racional de las pruebas que hayan sido practicadas.

⁴ Taruffo, Michele. (2010). *Simplemente la verdad: el juez y la construcción de los hechos*. Madrid: ed. Marcial Pons. Pág. 89 y ss.

⁵ STC 51/1985, de 10 de abril de 1985, F.J.2º (RTC 1985\51).

⁶ Ferrer Beltrán, Jordi. (2007). *La valoración racional de la prueba*. Madrid: ed. Marcial Pons. Pág. 54.

⁷ STC 208/2007, de 24 de septiembre, (RTC 2007\208).

⁸ Conclusión extraída de la lectura de la SAP de Valencia núm. 30/1999, de 1 de febrero, F.J. 1º y 2º (ARP 1999\921).

De no ser así se estaría sustrayendo al derecho a la prueba toda su virtualidad y eficacia. Ello está reforzado por el deber constitucional (art.120.3 CE) que tiene el juez de motivar las sentencias y que ha sido integrado dentro del derecho a la tutela judicial efectiva proclamada en el art. 24.1.CE por el TC, el cual ha estimado que puede prosperar un recurso de amparo por infracción del derecho a la utilización de los medios de prueba pertinentes por falta de motivación o si ésta es insuficiente o incoherente⁹.

⁹ STC 325/1994, de 12 de diciembre, F.J. 2º (RTC 1994\325).

3. LA PRUEBA DIGITAL O ELECTRÓNICA: LOS NUEVOS SISTEMAS DE COMUNIACIÓN DIGITAL.

3.1. Régimen normativo de la prueba electrónica.

3.1.1. La Ley de Enjuiciamiento Criminal y su vinculación con la LEC 1/2000.

Actualmente no existe una regulación específica sobre la prueba electrónica en la Ley de Enjuiciamiento Criminal¹⁰, sino que de forma frecuente han de aplicarse las normas que la misma contiene para materias análogas, teniendo siempre como referencia la doctrina que la jurisprudencia va produciendo.

La prueba electrónica es un medio de prueba autónomo, distinto del resto de medios de prueba, nacido por el avance de la tecnología en el ámbito de la información y comunicación, que es reconocido como tal dentro del procedimiento civil¹¹, pero no en el proceso penal, que como hemos subrayado carece de regulación específica en relación a la obtención, incorporación y valoración probatoria de este tipo de pruebas.

De conformidad con lo dispuesto en el art. 4 CC la legislación civil será de aplicación analógica en lo no previsto por las leyes penales. Por ello, se ha de tener presente el artículo 299.2 LEC, el cual reconoce como verdaderas fuentes de prueba los “medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase”, estas fuentes de prueba dan lugar al medio de prueba que se denomina “de la reproducción de la palabra, el sonido y la imagen y los instrumentos que permiten archivar y conocer datos relevantes para el proceso (art. 382-382LEC).

Con esta regulación, el legislador intentó adecuar los medios de prueba admisibles en el proceso civil al actual estado de la técnica, puesto que la LEC de 1881 no lo contemplaba de forma alguna. Sin embargo, no consideró la instrumentalización

¹⁰ Las únicas normas reguladas en la LECrim, por lo que se refiere al uso de medios electrónicos son las relativas a la declaración por video conferencia y a la documentación del juicio oral.

¹¹ El art. 299.2 LEC 1/2000 introduce esta novedad respecto el art. 578 de la LEC de 1881.

procesal de los adelantos científicos que posteriormente han ido apareciendo en nuestra vida cotidiana como tabletas, Smartphone, comunicación vía WhatsApp, etc¹².

Pese a ello, la LEC junto a los medios de prueba tradicionales abre las puertas a otros diferentes medios de prueba, quizás ya existentes o en fase de experimentación en el momento presente, o, en cualquier caso, de aquellos otros que puedan aparecer en el futuro con la siguiente redacción en el apartado 3 del mismo art. 299: “cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias”.

En conclusión, se implanta a través de esa redacción un *numerus apertus* en esta materia que da cabida a la utilización de los medios electrónicos como pruebas dentro del proceso judicial.

3.1.2. Normas sustantivas en relación con la prueba electrónica.

Si bien la norma jurídica que regula el proceso penal es la LECrim, (con el ya mencionado problema de insuficiencia de contenido por lo que a la prueba electrónica se refiere), también existen otras normas jurídicas nacidas en nuestro ordenamiento por la necesidad de regular los nuevos sistemas telemáticos de comunicación que han ido surgiendo en los últimos años. Estas normas estipulan el marco jurídico en el que deben desarrollarse las nuevas tecnologías y, por tanto, deben ser tenidas en cuenta a efectos de la obtención, incorporación y valoración de la prueba electrónica.

A) Normativa internacional:

A escala mundial no existen unos criterios homogéneos que regulen el uso de las nuevas tecnologías como fuente de prueba dentro del proceso. Ha sido a través de la Organización de las Naciones Unidas (ONU) que se ha promovido su regulación. Al respecto encontramos la siguiente normativa:

- *Resoluciones 55/63 y 56/121 adoptadas por La Asamblea General de la ONU. Sobre el combate contra el mal uso de las nuevas tecnologías de la información.*

¹² López Simó, Francisco. Ob. Cit. Pág. 21.

- *Recomendaciones aprobadas en el año 1985 por la CNUDMI*. Dirigidas a los gobiernos y a las organizaciones internacionales acerca del valor jurídico de los registros de ordenador.
- *Convención de la ONU (Nueva York, 2005)*. Sobre la utilización de las comunicaciones electrónicas en los contratos internacionales

B) Normativa comunitaria:

En nuestro ámbito comunitario coexisten dos modelos en relación con los requisitos que deben reunir las pruebas para su admisibilidad, por un lado, los que siguen un criterio muy amplio y que se basan en la libre consideración del juez para admitir o no la prueba electrónica, como son Austria, Dinamarca, Suecia, y Finlandia; y por otro lado, los países que tienen un criterio más restrictivo y que se remiten a los requisitos exigidos para los medios de prueba clásicos o tradicionales como son España, Francia e Italia.

- *Convenio Europeo de Derechos Humanos*. Su art. 8.1 recoge el derecho al respeto a la vida privada y familiar, al domicilio y a la correspondencia, art. 8.2 restringe la intervención del Estado, salvo por una serie de causas.
- *Convenio de Budapest sobre Ciberdelincuencia de 23 de noviembre de 2011*. Resulta aplicable no solamente a los denominados delitos informáticos, sino también “a la obtención de pruebas electrónicas de cualquier delito”.
- *Directiva 1999/93/CE*. Por la que se establece un marco comunitario y unitario para la firma electrónica.
- *Decisión marco 2005/222/JHA del 24 de febrero de 2005*. Relativa a los ataques de los que son objeto los sistemas de información y que tiene por objeto luchar contra la delincuencia informática y promover la seguridad de la información
- *Resolución AG-2008-RES-08 aprobada por la Asamblea General de la OIPC-INTERPOL, en su 77ª reunión, tenida lugar en San Petesburgo del 7 al 10 de*

octubre de 2008. Aprueba definir e impartir una formación adecuada a las unidades policiales intervinientes, así como coordinar misiones de apoyo en materia de informática forense, elaborar normas internacionales que regulen la búsqueda, el decomiso y la investigación de pruebas electrónicas, y seguir explorando la cooperación en este ámbito.

C) Normativa estatal:

En la última década, dentro del estado español se ha producido un notable aumento de la legislación respecto al uso de las nuevas tecnologías. En nuestro ordenamiento jurídico existe la siguiente normativa reguladora:

- *Ley 11/2007, de 22 de junio, sobre el Acceso Electrónico de los Ciudadanos a los Servicios Públicos.*
- *Ley 56/2007, de 28 de diciembre, de Impulso de la Sociedad de la Información.* Establece, aparte de otros aspectos relativos a la prestación de servicios de la sociedad de la información y la problemática de su conciliación con el imperativo de la protección de datos.
- *Ley 59/2003, de 19 de diciembre, de firma electrónica.* En ella se delimita y regula el uso de la llamada firma electrónica.
- *Ley 25/2007, de 18 de octubre, de Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.* Señala los datos necesarios para rastrear e identificar el origen, destino, fecha hora y duración de la comunicación.
- *Ley 34/2002, de 11 de julio, de Sociedad de servicios de la información.* Admite como prueba documental "el soporte electrónico en que conste un contrato celebrado por vía electrónica"
- *Ley 41/2007, de reforma del mercado inmobiliario.* Modifica el Artículo 318 de la LEC dándole una nueva redacción e incorporando la mención a "documento electrónico" en su Disposición Final Sexta.

- *Propuesta de Texto articulado de Ley de Enjuiciamiento Criminal elaborada por la comisión institucional creada por acuerdo del consejo de ministros de 2 de marzo de 2012, editado por el ministerio de justicia, Madrid, 2013.* Regula el “Registro de dispositivos de almacenamiento masivo de información” (arts. 347 y ss.) y “Registros remotos sobre equipos informáticos” (arts. 350 y ss.).

3.2. La necesaria adecuación de la legislación procesal a una nueva era.

Actualmente la informática ha adquirido un protagonismo absoluto en la vida de los ciudadanos y está presente en todos los ámbitos de las personas, ya sea en la esfera de sus relaciones laborales, afectivas, domésticas, educativas, etc. Tal circunstancia ha tenido un gran impacto en el mundo jurídico, pues aparatos y sistemas tecnológicos como puedan ser ordenadores o teléfonos móviles han abierto la puerta a la comisión de los llamados “delitos informáticos” así como también han servido para probar los hechos dentro de un proceso judicial, es decir, han dado paso a las llamadas “pruebas electrónicas”¹³.

Si bien se ha llevado a cabo una labor legislativa importante respecto a los delitos informáticos y su tipificación en el CP, no ha ocurrido lo mismo respecto a las pruebas electrónicas. Estas últimas tal y como se ha expuesto en el punto anterior carecen de regulación en la LECrim, no existe procedimiento específico alguno que regule la obtención, conservación y presentación de la prueba electrónica ante los Tribunales españoles, hecho que hace mover los cimientos de la seguridad jurídica en los que se asienta nuestra constitución.

En esa línea, y después de que España ratificara el Convenio de Budapest sobre Ciberdelincuencia de 23 de noviembre de 2011¹⁴, es precisa la introducción en la Ley de Enjuiciamiento Criminal de una regulación específica acerca del acceso y obtención de la información contenida en dispositivos electrónicos así como su incorporación y

¹³ Abel Lluch, Xavier. (2012). *Derecho probatorio*. Madrid: ed. Bosch Procesal. Pág. 939-941.

¹⁴ El Convenio de Budapest sobre Ciberdelincuencia de 23 de noviembre de 2011, resulta aplicable a los denominados delitos informáticos, así como a “la obtención de pruebas electrónicas de cualquier delito” de acuerdo con su art. 14.2 c).

valoración en el proceso penal, para asegurar un procedimiento con pleno respeto a las garantías del proceso.

Es necesario también tener en cuenta que la Ley no puede regular de forma específica cada uno de los aspectos de esta compleja materia, sino que ha de existir una normativa reglamentaria, así como una protocolización u homologación de actuaciones que regule pormenorizadamente las formas de acceso a las pruebas electrónicas, los pasos a seguir en la realización de las pruebas periciales y las singularidades de la cadena de custodia para garantizar su autenticidad e integridad.

3.2.1. Las tecnologías de la Información y de las Comunicaciones.

Las ventajas que ofrecen las tecnologías de la información y de las comunicaciones (TIC) han fomentado su rápida implementación en todos los hogares. El actual uso generalizado de los nuevos sistemas tecnológicos ha conllevado una modificación sustancial de la forma de actuar de los ciudadanos y organizaciones por lo que se refiere a la producción y tratamiento de la información así como a la forma de comunicación.

Si bien el uso de las TIC facilita, agiliza y dinamiza la comunicación también conlleva riesgos y amenazas que hasta ahora no existían, como son la perpetración de los delitos que se sirven de las nuevas tecnologías.

En este sentido, la prueba electrónica se presenta como una herramienta fundamental para resolver potenciales casos de infracción, fraude o delito en los que existan dispositivos electrónicos involucrados o que hayan sido cometidos a través de los mismos¹⁵.

Pese a la existencia de esta herramienta, la ausencia de procedimientos legales específicos provoca una gran inseguridad jurídica, haciendo necesaria una interpretación de las normas procesales existentes, de la jurisprudencia y de la doctrina para saber cómo realizar la obtención, el análisis y la presentación de las pruebas electrónicas dentro del proceso judicial. Ello es muy importante, puesto que, si se hace de forma

¹⁵ Tal y como expone Calderón Cuadrado, M^a Pía sobre la sociedad de la información y modernización de la justicia, en su obra (2011). *La encrucijada de una justicia penal tecnológicamente avanzada*. Madrid: ed. La Ley. Pág.25.

correcta se adoptaran las medidas técnicas concretas más idóneas que garanticen la autenticidad, integridad y futura admisibilidad de las pruebas electrónicas en un procedimiento judicial.

3.2.2. La relevancia probatoria de los soportes informáticos.

Dado que la principal función de la prueba es ofrecer al Juzgador información que pueda ser útil para establecer la verdad de los hechos en litigio, las partes pueden presentar todos los medios de prueba que sean lo suficientemente relevantes para ofrecer una base cognitiva que establezca la verdad de un hecho en litigio¹⁶.

Frente a los tradicionales medios de prueba aparece una herramienta que permite acreditar la realización de actos, acuerdos y comunicaciones frente a la justicia: la prueba electrónica. Este instrumento está ganando cada vez más peso en los procesos judiciales; de tal forma que puede afirmarse que muchas pruebas tradicionales presentadas en juicio están migrando desde el soporte de papel hacia un entorno virtual. La prueba electrónica puede materializarse a través de un sinfín de medios como USB, mensajes de texto a través de e-mails, SMS, WhatsApp, grabaciones de vídeo, audio, etc. Todos ellos pueden devenir relevantes dentro de un proceso y ser claves para demostrar la veracidad o falsedad de los hechos controvertidos en el mismo.

El concepto de relevancia es especialmente importante como criterio para la selección de los medios de prueba admisibles. La relevancia es un estándar lógico de acuerdo con el cual los únicos medios de prueba que deben ser admitidos y tomados en consideración por el juzgador son aquellos que mantienen una conexión lógica con los hechos en el litigio, de modo que pueda sustentarse con ellos una conclusión acerca de la verdad de tales hechos¹⁷.

Si bien la práctica de la prueba es un derecho constitucional, la doctrina del TC existente al respecto ha dejado claro los siguientes extremos: este derecho fundamental atribuye sólo el derecho a la recepción y práctica de las pruebas que sean pertinentes, se hayan solicitado en la forma y momento legalmente establecidos, siendo sólo

¹⁶ STC 37/2000, de 14 de febrero, F.J. 3. (RTC 2000\37).

¹⁷ López Simó, Francisco. Ob. Cit. Pág. 86-90.

admisibles los medios de prueba autorizados por el ordenamiento. Les corresponde a los Jueces y Tribunales el examen sobre la legalidad y pertinencia de las pruebas¹⁸.

Pese a la importancia que adquieren los nuevos sistemas electrónicos para esclarecer la verdad acerca de los hechos controvertidos dentro de un proceso judicial, dada la naturaleza singular de los datos almacenados en estos sistemas y dispositivos así como las importantes diferencias existentes entre esos datos y los documentos escritos, surge la problemática acerca de cómo establecer los límites de admisibilidad como pruebas judiciales, cómo se pueden reunir y representar y qué valor probatorio pueden alcanzar¹⁹.

3.3. Tratamiento doctrinal de la prueba electrónica.

3.3.1. Concepto

Cuando en materia penal se hace referencia a la prueba electrónica, se está hablando de un medio encaminado a convencer al juez sobre la existencia de un hecho punible, mediante el rastro de hechos e informaciones contenidas en medios electrónicos tales como las grabaciones en sistemas de vídeo o cámaras, grabaciones de audio, mensajes de texto en teléfonos móviles, archivos electrónicos almacenados en discos duros, USB, disquetes, Smartphone o tabletas entre otros²⁰.

Así, la prueba electrónica es toda información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio, que sirve para adquirir convencimiento de la certeza de un hecho²¹. Dentro de este concepto de prueba electrónica cabe distinguir entre lo que es almacenaje de los datos e informaciones en un dispositivo electrónico, de lo que es la transmisión de esos datos o informaciones a través de las distintas redes de comunicación existentes, como por ejemplo Internet o telefonía móvil.

¹⁸ STC núm. 168/2002, de 30 septiembre, F.J.2º (RTC 2002\168), en el mismo sentido la STC núm.71/2003 de 9 abril, F.J. 3º (RTC 2003\71) y la STC núm. 1/2004 de 14 de enero, F.J. 2º (RTC 2004\1).

¹⁹ Taruffo, Michelle. (2008). *La prueba*. Madrid: ed. Marcial Pons. Pág. 85.

²⁰ Cabezudo Rodríguez, N. (2004). *Omisiones del legislador procesal ante los medios de prueba tecnológicos*. Madrid: ed. La Ley. Pág. 1703.

²¹ Definición dada en la Decisión 2002/630/JAI del Consejo, de 22 de julio de 2002, relativa a la cooperación policial y judicial en materia penal (AGIS), Diario Oficial L 203 de 1 de agosto de 2002.

La naturaleza electrónica de la prueba implica la utilización de un lenguaje binario a través de un sistema que transforma impulsos o estímulos eléctricos fotosensibles y, por cuya descomposición y recomposición informática grabada en un formato electrónico, genera y almacena la información. Dicho lenguaje es un código ininteligible para aquellas personas que no sean informáticos. La visualización del texto en pantalla es una mera traducción en lenguaje alfabético común, descodificado²².

Frente a las pruebas tradicionales, de acuerdo con Manuel M. Gómez del Castillo y Gómez, la prueba electrónica tiene las siguientes características:

- **Intangibles:** Las evidencias electrónicas se encuentran en formato electrónico, siendo reproducibles, de fácil copia, diluyéndose las posibilidades de distinguir los originales de las copias.
- **Volátiles:** Las evidencias electrónicas son mudables, inconstantes, en definitiva, manipulables, por lo que pueden ser modificadas.
- **Delebles o destruibles:** Las evidencias electrónicas pueden ser borradas o incluso cabe la posibilidad de que los soportes en los que se almacenan sean destruidos.
- **Parciales:** Normalmente, aunque no siempre es así, las evidencias electrónicas se encuentran en soportes que están en poder de quien las presenta como argumento de las pretensiones alegadas.
- **Intrusivas:** En ocasiones la recogida de las evidencias electrónicas puede afectar los derechos y libertades fundamentales de las personas como, entre otros, el derecho a la intimidad, el secreto de las comunicaciones, la libertad sindical o la protección de datos de carácter persona²³.

²² Abel Lluch, Xavier (dir); Ginés Castellet, Núria (coor.). (2006). *Empresa y prueba informática*. Barcelona: ed. Bosch Editor. Pág. 23.

²³ Artículo doctrinal de Gómez del Castillo y Gómez, Manuel. (2009). *Aproximación a los nuevos medios de prueba en el proceso civil*. Revista "Derecho y conocimiento" de la Facultad de derecho de la Universidad de Huelva. Pág. 5-12.

3.3.2. Valor probatorio

La aportación de pruebas electrónicas a un proceso plantea dudas acerca de cuándo pueden ser empleados estos medios y cuál es su valor probatorio para los jueces y magistrados.

Una cosa es que puedan aportarse como prueba y otra es el valor que puede otorgársele a la prueba en cuestión, ello dependerá de las garantías que se tengan de si han podido ser manipuladas. Por ello es de vital importancia que exista autenticidad e integridad en los dispositivos electrónicos que se intentan utilizar como prueba.

3.3.2.1. La garantía de la autenticidad e integridad de la prueba.

El respeto por la legalidad en la obtención de la prueba tiene un papel fundamental a la hora de valorar la admisibilidad de la misma. De forma más concreta, la cadena de custodia adopta una serie de singularidades cuando se aplica a las pruebas electrónicas, puesto que si se realiza de forma regular, de acuerdo con la ley y el protocolo de actuación, aportará mayor seguridad a la actuación de los distintos sujetos del sistema penal y reducirá el margen de error en sus actuaciones, limitando el riesgo de contaminación o alteración de la autenticidad e integridad de las pruebas²⁴.

De conformidad con lo dispuesto en el artículo 230.2 de la LOPJ, resulta necesario asegurar la autenticidad y la integridad de la prueba electrónica incorporada al proceso, es decir, garantizar la fuente de la que proceden y que el activo de la información no ha sido alterado de manera no autorizada, de tal manera que quede asegurado que la sometida al tribunal de enjuiciamiento es la misma que la que fue incautada o aprehendida²⁵.

Serán importantes los conocimientos del juez y contar con el auxilio técnico de un perito informático, para comprobar que el modo en el que se incorporan estos soportes al proceso cumple con la licitud, autenticidad e integridad requeridas para que sea posible su valoración como prueba electrónica.

²⁴Abel Lluch, Xavier. (2012). *Derecho probatorio...* Ob.Cit. Pág. 941-944.

²⁵ Respecto a la importancia de constatar la autenticidad de la prueba, la STS, Sala 1ª, de 30 de noviembre de 1981, F.J. 2º (RJ 1981/4680) no admite que puedan aportarse como medio de prueba unas cintas magnetofónicas debido a la dificultad de comprobar la autenticidad de la grabación, fundamentando la negativa en el carácter cerrado de los medios de prueba entonces vigentes art. 578 LEC 1881 y 1215 CC.

Si bien es cierto que cuando las pruebas electrónicas se admiten como medios de prueba debe estimarse su valor probatorio, en general, se puede decir que éste es estimado discrecionalmente por el juzgador y que, un dispositivo digital como lo es un correo electrónico no tiene la fuerza vinculante de algunos documentos especiales regulados específicamente por el derecho como lo es un documento notarial. El soporte técnico, por un lado, y las garantías de autenticidad, por otro, completan el cuadro de factores que más influyen en los órganos juzgadores europeos a la hora de conceder mayor o menor valor probatorio a una determinada prueba²⁶.

Por tanto, el valor probatorio de las pruebas electrónicas en los tribunales españoles, queda regulada a través de disposiciones generales aplicables a la prueba tradicional, sin que, hasta el presente, exista ninguna regulación nacional específica. Todo ello hace que la percepción en el proceso de obtención, presentación y admisión de las pruebas electrónicas de cara a un juicio, junto con el vacío legislativo dominante, generan cierta inseguridad jurídica y profesional.

3.3.2.2. El juicio de licitud. El respeto a los derechos fundamentales.

La viabilidad procesal de la prueba electrónica está conectada a un previo juicio de licitud, es decir, que la prueba se haya obtenido sin violar los derechos fundamentales, en otro caso, sería nula de acuerdo con lo regulado en el artículo 11.1. LOPJ.

La versatilidad tecnológica que han alcanzado los instrumentos electrónicos les convierte en herramientas indispensables en la vida cotidiana con múltiples funciones que hacen que el acceso a la información contenida en los dispositivos electrónicos pueda afectar a varios derechos fundamentales.

²⁶ Taruffo, Michelle. (2008). *La prueba...* Ob.Cit. Pág.89.

En este sentido, los derechos fundamentales que pueden verse perjudicados son:

A) El derecho a la intimidad personal recogida en el art. 18.1CE puede verse dañado.

Únicamente es legítima la injerencia si concurre la autorización judicial previa o bien el consentimiento del afectado²⁷. Aunque no cabe descartar la posible intervención policial en aquellos casos de urgente necesidad siempre que sea con respeto al principio de proporcionalidad²⁸.

B) El derecho al secreto de las comunicaciones recogido en el art. 18.3CE puede sufrir una intromisión.

Esto ocurre en los casos en que se tenga acceso a datos que formen parte de un proceso de comunicación, es decir, que se desvelen procesos comunicativos. Debemos tener en cuenta que si la información se refiere a una comunicación ya terminada o consumada, en principio solamente existiría una injerencia en el derecho a la intimidad, si bien en determinados supuestos la jurisprudencia puede entender afectado el derecho al secreto de las comunicaciones también²⁹.

C) El derecho a la inviolabilidad domiciliaria recogido en el art. 18.2CE puede verse lesionado.

Ello sucede en el caso de que el dispositivo electrónico se encuentre en el interior de un lugar cerrado entendido como domicilio³⁰.

3.4. Clases

A) CORREO ELECTRÓNICO.

Esta fuente de prueba electrónica puede ser un mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que éste acceda al mismo³¹.

²⁷ Tal y como expone la STC 173/11 de 7 de noviembre, F.J. 5º (RTC 2011\173).

²⁸ Como expone la STC 115/2013, de 9 de mayo, F.J. 3º (RTC 2013\115).

²⁹ De acuerdo con la la STC 115/2013, de 9 de mayo, F.J. 4º (RTC 2013\115).

³⁰ Un ejemplo de lesión del derecho a la inviolabilidad domiciliaria es la STC 161/1999, de 27 septiembre, recurso de amparo núm. 2294/1995 (RTC 1999\161).

La ley de Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de las comunicaciones descompone el correo electrónico en dos partes: el mensaje con sus anexos (fotos, vídeos, audios, etc.) y los datos de tráfico, que son aquellos que suelen estar en la cabecera del correo y nos indican cuál es su destino, origen, fecha, hora, duración, tipo, equipo y localización de la comunicación³².

Siguiendo lo estipulado en el art. 334 de la LECrim el correo electrónico debe ser recogido y conservado por el Secretario Judicial. Para el caso en el que el correo electrónico no esté en el ordenador, sino en el servidor, el Secretario Judicial deberá abrirlo y pasarlo al disco duro precintándolo después para evitar su manipulación o borrado. Posteriormente, deberá hacerse un clonado o volcado en copias del disco duro, copias sobre las que trabajaran los peritos, para evitar que el original sea alterado.

De acuerdo con la jurisprudencia, para que la copia sea valorada como prueba de cargo es necesario que se garantice que lo encerrado en esa copia es lo mismo que lo contenido en la original, debiendo para ello indicarse si se han traducido los mensajes acompañar los traducidos con los originales, expresando los datos necesarios para permitir su lectura y que puedan ser sometidos a contradicción sobre su veracidad y autenticidad por las partes que la nieguen³³.

Es necesario tener en cuenta algunos aspectos problemáticos que conlleva la incorporación en el proceso del correo electrónico como medio de prueba.

En primer lugar, es difícil determinar la autoría o participación por parte del emisor, puesto que es posible averiguar el origen físico del correo pero no la persona que lo ha escrito o enviado. De igual forma, se presentan problemas con la autoría o participación por parte del receptor.

En segundo lugar, existen dificultades para obtener los datos de tráfico o intervenir los contenidos de los correos cuando la empresa utilizada tenga sede en Estados Unidos, como por ejemplo Gmail o Yahoo!, puesto que su legislación³⁴ exige pedirlos a través

³¹ Art. 2.h) Directiva 58/2002/CE, de 12 de julio.

³² Art. 3 de la Ley 25/2007, de 18 de octubre, de Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

³³ Sentencia dictada en la Operación Tigris por la AN 31/2009, de 30 abril (JUR 2009\244859).

³⁴ Básicamente lo contenido en Electronic Communications Privacy Act (ECPA) de 1986, la cual fue promulgada por el Congreso de Estados Unidos para extender las restricciones del gobierno sobre escuchas telefónicas de llamadas telefónicas para incluir las transmisiones de datos electrónicos por ordenador.

de Comisión Rogatoria, que se trate de delitos graves como el terrorismo o el crimen organizado y el plazo legal que tienen de conservación de esos datos es muy corto.

En tercer lugar, existen problemas de competencia de los Tribunales españoles en caso de que los correos ilícitos estén almacenados en un servidor extranjero. Este problema ha sido solucionado en parte por el Acuerdo del Pleno no jurisdiccional de la sala II del Tribunal Supremo de 03/02/2005 estableciendo que "El delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo. En consecuencia, el Juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales será en principio competente para la instrucción de la causa"³⁵.

Por último, cabe resaltar la obligación legal por parte del Juez de perseguir los delitos heterogéneos que se conozcan y surjan durante la instrucción atendiendo a su flagrancia patente y la regla de conexidad de los arts. 17.5 y 300 LECrim³⁶.

B) MENSAJE DE TELÉFONO (SMS Y WHATSAPP).

El mensaje de teléfono se emplea para enviar y recibir mensajes de texto. Se trata de una prueba electrónica que podemos encontrar en diversas versiones, como por ejemplo son los mensajes SMS, los cuales contienen una cadena alfanumérica de hasta 140 caracteres o de 160 caracteres de 7 bits, y cuyo encapsulado incluye una serie de parámetros. También existen los mensajes vía WhatsApp Messenger, es decir, a través de una aplicación de mensajería multiplataforma que permite enviar y recibir mensajes sin pagar por SMS.

A este tipo de prueba electrónica le es aplicable todo lo analizado respecto al correo electrónico sobre su recogido y conservación. Presenta una gran problemática acerca de su valoración por los tribunales por su fácil su manipulación y por la dificultad de probar la autoría de los mensajes.

Sobre esta problemática la jurisprudencia no es unánime a la hora de resolver, puesto que encontramos sentencias divergentes en su argumentación, como la sentencia de la

³⁵ En la misma línea encontramos como jurisprudencia que desarrolla ese acuerdo la STS núm. 341/2005, de 17 de marzo, (RJ 2005\3561).

³⁶ Respeto al descubrimiento casual de otro delito se pronunciar la STS núm. 651/1996, de 4 de octubre (RJ 1997\816), así como la STS núm. 1611/1997, de 29 de diciembre, (RJ 1997\9098), la STS núm. 1311/2000, de 21 julio, (RJ 2000\6917) y la STS núm. 992/2003, de 3 julio, (RJ 2003\6153).

AP de Madrid 12/2013 que otorga valor probatorio a mensajes WhatsApp³⁷, mientras que otras sentencias como la Sentencia AP de Cádiz 31/2014 no acepta como prueba mensajes telefónicos por no poderse comprobar su autoría y manipulación³⁸, la sentencia AP de Pontevedra 10/2014, tampoco acepta como prueba mensajes telefónicos por el desconocimiento de la titularidad del teléfono³⁹, o la Sentencia AP de Madrid 1260/2012, la cual considera fácilmente manipulable el contenido de un mensaje telefónico⁴⁰.

Además del problema de manipulación y autoría de estos mensajes, actualmente es muy frecuente el uso de la mensajería telefónica para cometer delitos como injurias, amenazas o acoso. Ello hace que en numerosas ocasiones la víctima se dirija a dependencias policiales o judiciales con su terminal, el cual puede recogerse como cuerpo del delito aunque en la mayoría de ocasiones se hace una transcripción a papel de los mensajes para incorporarlos al proceso. En caso que la aportación sea por un

³⁷ A este respecto la sentencia de la Audiencia Provincial de Madrid, estableció en la sentencia número 12/2013 de 5 abril. (JUR 2013\175198) que " los mensajes, enviados a través del WhatsApp, que han resultado transcritos en el Juzgado de Violencia Sobre la Mujer nº 3 de Madrid, al inicio de las actuaciones judiciales que, como ya anticipábamos adquieren un singular valor probatorio, porque, tanto por la secuencia horaria en que las comunicaciones entre Celia y Concepción se realizan, como por el contenido de las mismas, suponen un elemento de corroboración objetiva puntual y exacta de lo declarado, coincidentemente, por las dos testigos

³⁸ En este sentido, encontramos la sentencia de la Audiencia Provincial de Cádiz, número 31/2014 de 28 enero. (JUR 2014\95996) la cual motiva su decisión de la siguiente forma: "*pues no habiendo declarado los dos implicados, de la existencia de lesiones no puede desprenderse el origen de su autoría y unos mensajes de wasap sobre los que ningún técnico ha declarado y que no consta que sean veraces o emitidos por el apelante o que no hayan podido ser manipulados, no es suficiente prueba para sustentar en ella el pronunciamiento condenatorio que se combate, razón que hace procedente la estimación del recurso [...]*".

³⁹ La sentencia de la Audiencia Provincial de Pontevedra, número 10/2014 de 10 enero. (JUR 2014\25448) interpreta que "*la prueba que sustenta la condena del recurrente, aparte del dato objetivo de la existencia de los carteles y WhatsApp, de indiscutible carácter vejatorio y ofensivo, se deriva de las manifestaciones de la denunciante, pues no consta siquiera la titularidad del teléfono desde el que se envían los mensajes y las declaraciones de los testigos no son concluyentes. Tales datos, se estima son manifiestamente insuficientes para deducir de ellos, con el nivel de certeza necesario para sustentar una Sentencia condenatoria [...]*".

⁴⁰ Sobre la posible manipulación, la sentencia de la Audiencia Provincial de Madrid, número 1260/2012 de 1 octubre. (JUR 2012\341849) se expresa de la siguiente forma: "*También considera que el contenido las WHAT'S APP son fácilmente manipulables, y se pueden borrar parte las conversaciones, por lo que entiende que el libre acceso que han tenido los agentes a estas WHAT'S APP, contactos y todo tipo de aplicaciones del teléfono móvil del terminal de don Elias vulneran el artículo 18,3 de la Constitución y por lo tanto considera que debe existir una nulidad de todas las transcripciones y los pantallazos incorporados a las actuaciones [...]*".

tercero sólo será una prueba electrónica lícita si éste demuestra que le ha sido cedido legítimamente por una de las partes de la conversación.

En estos casos el Secretario Judicial es el encargado de realizar el cotejo entre las transcripciones y el texto original, tal diligencia constituirá una prueba documental pre constituida.

C) PÁGINA WEB

La página web, también llamada página electrónica o ciberpágina, es un documento o información electrónica capaz de contener texto, sonido, vídeo, programas, enlaces, imágenes, adaptada para la llamada World Wide Web, y que puede ser accedida mediante un navegador. A través de estas páginas incluidas en Internet normalmente se informe sobre productos o actividades de personas físicas o jurídicas.

La problemática que plantea esta herramienta electrónica es la determinación de quién es el responsable del contenido. Actualmente este problema se ve patente en los comentarios alojados en las páginas web susceptibles de ser ilícitas o lesionar y afectar a derechos fundamentales, como por ejemplo son los cada vez más frecuentes comentarios vejatorios.

A este respecto, si bien no existe por parte del prestador de servicios, obligación alguna de supervisar o fiscalizar apriorísticamente los comentarios vertidos en su página web, sí existe la obligación de ofrecer una información detallada y accesible para poder contactar con él, a fin de que retire los comentarios vejatorios⁴¹. El prestador no es responsable de lo publicado por otros usuarios cuando no tenga un conocimiento efectivo⁴² del contenido vejatorio notorio y evidente, y cuando habiendo tenido conocimiento del mismo, con premura haya procedido a suprimirlo.

D) REGISTRO FONOGRAFICO, VIDEOGRABACIÓN, FOTOGRAFÍA DIGITAL.

Se trata de la reproducción de sonidos o imágenes, datos, cifras u operaciones matemáticas captadas a través de instrumentos de filmación, grabación o semejantes que

⁴¹ De acuerdo con la SAP Madrid núm. 46/2011, de 10 febrero, F.J. 2º (JUR 2011\161073).

⁴² La jurisprudencia ha interpretado de manera extensiva “conocimiento efectivo” entendiéndolo por aquel que provenga de cualquier otro medio fehaciente, sin necesidad de previa declaración de ilicitud, lo vemos en la STS núm. 1295/2009 de 9 diciembre. F.J. 3º (RJ 2010\303), la STS núm. 492/2010 de 18 mayo F.J. 1º (RJ 2010\5814) y la SAP Madrid núm. 362/2011 de 25 abril. (JUR 2011\249542).

quedan registradas en soportes técnicos como cintas de vídeo, discos magnéticos, cámaras digitales, etc.

Este tipo de prueba presenta menos problemas que las pruebas descritas anteriormente puesto que tienen una regulación más específica que dibuja de forma más clara el camino a seguir durante el proceso. Si bien los problemas más frecuentes son en relación a la vulneración de derechos fundamentales en su consecución⁴³ y su posible manipulación, pero no plantean demasiados problemas respecto a su autoría, la cual en la mayoría de ocasiones no es relevante.

E) DISPOSITIVOS ELECTRÓNICOS DE ALMACENAMIENTO.

Respecto a los dispositivos de almacenamiento éstos son dispositivos que sirven para grabar datos de forma permanente o temporal, los cuales pueden ser USB, discos duros, DVD, CD, etc. El medio probatorio propuesto puede ser el examen judicial de palabras, textos, cifras y operaciones matemáticas que se encuentren almacenados en los correspondientes soportes técnicos.

Existe en este tipo de prueba electrónica la misma problemática: averiguar quiénes son los autores de los datos que en los dispositivos de almacenamiento se contienen y si éstos han sido manipulados.

F) DOCUMENTOS ELECTRÓNICOS.

La prueba basada en un documento electrónico es aquella que se basa en un documento que tiene como soporte material algún tipo de dispositivo electrónico o magnético, cuyo contenido se encuentra codificado a través de algún tipo de código digital el cual puede ser interpretado, reproducido o leído mediante detectores de magnetización⁴⁴.

El problema que presenta el documento electrónico contenido en los dispositivos de almacenamiento, como puede ser una hoja de Excel, es su inmaterialidad⁴⁵. Mientras que el texto escrito en papel es, realmente, un documento que enseña lo que contiene, y

⁴³ A título de ejemplo la SAP Córdoba núm. 136/2002, de 25 mayo, (AC 2002\1000) sobre reproducción de imágenes grabadas y derecho a la intimidad.

⁴⁴ A este respecto podemos citar la STS, de 12 de diciembre de 1988, (RJ/9435) que define los documentos como aquellos en que hay constancia “generalmente escrita” o la STS, de 3 de julio de 1989 (RJ 1989/5283) en que se califican expresamente como documento privado unas fotografías.

⁴⁵ La STS, de 19 de abril de 1991, F.J. 4º (RJ 1991/2813) abogaba por superar un concepto del documento ceñido a la escrito motivando que “nuevas técnicas han multiplicado las ofertas de soportes: una grabación de vídeo, un disco, los disquetes informáticos...”

en él hay identidad entre lo grabado y lo exteriorizado, por el contrario, lo almacenado en soporte electrónico no se exterioriza, y en caso de que lo haga no existe identidad entre lo conservado y lo exteriorizado, puesto que lo conservado constituye un archivo en sistema binario, mientras que lo exteriorizado adopta la forma de escritura con las letras de nuestro alfabeto, pero son signos de escritura que no existen en la realidad natural, no tienen base material tangible, sino virtual.⁴⁶

La jurisprudencia más reciente se pronuncia a favor de un concepto amplio de documento en el que lo esencial es la transmisión de información y lo secundario el soporte en el que se recoge.

Así el TS expresa que “el soporte papel ha sido superado por las nuevas tecnologías de la documentación y la información. Cualquier sistema que permita elaborar ideas, declaraciones, informes o datos susceptibles de ser reproducidos en su momento, suple con ventajas al tradicional documento escrito, siempre que existan instrumentos técnicos que permitan acreditar la fiabilidad y Seguridad de los impresos en soporte magnético. Se trata de una realidad social que el derecho no puede desconocer. El documento electrónico imprime en las “neuronas tecnológicas”, de forma indeleble, aquello que se ha querido transmitir por el que maneja los hilos que transmiten las ideas, pensamientos o realidades de los que quiere que quede constancia. Su autenticidad es tan firme que supera la realidad que puede visualizarse en un documento escrito⁴⁷”.

⁴⁶ La STS, de 2 de diciembre de 2000, F.J. 2º (RJ 2000/9955) razona que el concepto de documento admite los plasmados por escrito, y aquellos otros que pueden ser asimilados, entre los que enumera, a modo ejemplificativo, un ordenador, un vídeo y una película.

⁴⁷ Motivación expresada en la STS, de 4 de noviembre de 2009, F.J. 2º (La Ley 226669/2009).

4. LA INCORPORACIÓN DE LA PRUEBA ELECTRÓNICA EN EL PROCESO

4.1. Formas de acceso.

Dada la gran variedad de instrumentos y elementos tecnológicos que tenemos a nuestro alcance, existe una gran heterogeneidad de las formas de acceder a su contenido, pudiendo distinguirse varias modalidades básicas respecto a la incorporación de la prueba digital o electrónica en el proceso.

En primer lugar, existe la posibilidad de que las partes sean las que realicen tal aportación, cuando sean las mismas las que tengan en su poder o custodia tales pruebas.

En segundo lugar, otra forma de acceso al contenido de la prueba electrónica es a través de la posesión material o física de la misma, no porque esté en poder de la parte que la quiere aportar sino porque haya sido aprehendida por la autoridad competente. Dentro de esta forma podemos distinguir por un lado, la aprehensión del propio dispositivo electrónico encontrado fuera de lugar cerrado y por otro lado, la diligencia de entrada y registro en lugar cerrado con ocupación del dispositivo o de la información relevante.

En tercer lugar, existe la posibilidad técnica de acceder al contenido de un sistema informático sin necesidad de realizar aprehensión física alguna, sino a través de los denominados registros remotos⁴⁸.

En cuarto lugar, también se puede acceder a la información contenido en un servidor o sistema que sea accesible a través de otro al cual se haya accedido de forma tradicional o por registro remoto, así por ejemplo acceder a un mensaje publicado en internet, desde la página en que se publicó⁴⁹.

En quinto lugar, existen especialidades respecto al llamado registro transfronterizo, es decir, aquel en el que los datos se encuentran en un sistema informático o servidor situado fuera del territorio nacional.

Es necesario tener en consideración que la preservación de datos y el volcado de información se deben realizar en atención a asegurar su autenticidad e integridad⁵⁰.

⁴⁸ Conocidos como *remote search*.

⁴⁹ Así la STS, de 9 de mayo de 2008, FJ 2º y 3º (RJ 2008/4648) admite la validez de los rastreos efectuados por la policía de los protocolos IPS (Internet Protocols) que identifican los ordenadores de los usuarios.

⁵⁰ Consideraciones estudiadas en detalle en el apartado 3.3.2. del presente trabajo.

4.2. En fase de instrucción.

El proceso penal comienza cuando se formula una acusación contra una persona determinada por un hecho criminal concreto, pero para poder llegar a ese punto se requiere de la realización de una serie de actos de investigación encaminados a averiguar las circunstancias del hecho y la personalidad de sus autores que fundamenten la posterior acusación⁵¹.

Por ello, existe una etapa o subfase inicial llamada de investigación, procedimiento preliminar o fase de instrucción. Si bien legalmente el procedimiento preliminar recibe el nombre de sumario, diligencias previas y diligencias urgentes, según se trate de un proceso penal ordinario por delitos más graves, un proceso penal abreviado o un proceso penal para el enjuiciamiento rápido de determinados delitos, respectivamente⁵².

Dentro de la fase de instrucción existen distintas formas de acceso al contenido de los diferentes instrumentos y elementos tecnológicos como fuente de prueba electrónica. Tal y como se ha expuesto en el apartado anterior, estas modalidades son: la aportación por las partes, la aprehensión de dispositivo fuera de lugar cerrado, diligencia de entrada y registro en lugar cerrado, los registros de información accesible y registros remotos.

4.2.1. Aportación de la prueba electrónica por las partes.

Las partes pueden ser las que aporten prueba electrónica al proceso solicitando la unión a los autos del dispositivo en el que se encuentra esa prueba, así como también pueden acompañar una copia en papel con la transcripción de la información relevante.

De igual forma, pueden solicitar al Juez la remisión de una prueba o documento electrónico, designando oportunamente el lugar o archivo en el que se encuentre. En este caso se podrá, a instancia de parte o de oficio, practicar algún examen pericial sobre la prueba electrónica de la que se trate⁵³.

⁵¹ Se desprende de la literalidad del art. 299 LECrim.

⁵² Montero Aroca, Juan; Gómez Colomer José Luis; Montón Redondo, Alberto; Barona Vilar, Silvia. (2013). *Derecho Jurisdiccional III, proceso penal*. (21ª edición). Valencia: Ed. Tirant lo Blanch. Pág.119.

⁵³ Castillejo Manzanares, Raquel. (2010). En *“Medios Probatorios”, dentro del libro “Hacia un nuevo proceso penal. Cambios necesarios”*. Madrid: ed. La Ley. Pág. 26.

Finalmente, la parte interesada podrá introducir la prueba electrónica en el juicio oral proponiéndola como alguno de los medios admitidos legalmente⁵⁴.

4.2.2. Aprehensión de dispositivo fuera de lugar cerrado.

Se trata de los supuestos en los que se realiza una aprehensión o incautación de un dispositivo electrónico que se halla fuera de un lugar cerrado, ya sea en un lugar abandonado o en poder de una persona. Existen tres supuestos en los que pueden ser ocupados o aprehendidos los dispositivos electrónicos:⁵⁵

- **Como instrumentos de delito.** Los dispositivos electrónicos son los medios u objetos a través de los cuales se perpetra el delito.
- **Como cuerpo del delito.** Los dispositivos electrónicos son la cosa objeto de la infracción penal o contra la que se ha dirigido el hecho punible.
- **Como piezas de convicción.** Se trata del resto de objetos, huellas y vestigios que tienen relación con el delito y pueden servir de prueba o indicio de la autoría y demás circunstancias del hecho punible.

Actualmente no existe una regulación legal que fije específicamente los pasos que deben seguirse en estos supuestos. Por ello, es necesario acudir a la jurisprudencia, la cual ha venido admitiendo la práctica de estos registros si bien con la necesaria observancia de los presupuestos para la injerencia en el derecho a la intimidad⁵⁶.

A) Fase de aprehensión o incautación del dispositivo.

Se trata del momento en el que el Juez de Instrucción o bien la Policía Judicial⁵⁷ recogen los dispositivos electrónicos que se presume contienen la información relevante para la acreditación de los elementos y circunstancias del delito. Estos dispositivos incautados deben quedar bajo responsabilidad del Secretario Judicial o conservados a disposición judicial en el organismo adecuado para su depósito, para que puedan incorporarse al proceso de forma legal (art. 338 LECrim).

⁵⁴ En este sentido, en el apartado 4.3. del presente trabajo se estudian de forma detallada cada uno de los medios de incorporación de la prueba electrónica en el proceso.

⁵⁵ De Diego Díez, Luis Alfredo. (2005). *Ocupación, conservación y destrucción de las piezas de convicción*. Valencia: Ed. Tirant lo Blanch. Pág. 18-20.

⁵⁶ Bonachera Villegas. (2012). *El registro de archivos informáticos: una cuestión necesitada de regulación*. En Revista General de Derecho Procesal 27. Pág.11.

⁵⁷ Funciones que ambos cuerpos tienen establecidas en los arts. 326.1º LECrim y 282 LECrim respectivamente.

B) Fase de acceso a la información contenida en su interior.

Cuando ya se ha aprehendido el dispositivo electrónico es necesario realizar un registro del dispositivo para inspeccionar los datos e información que éste contiene. Con esto se afecta al derecho fundamental a la intimidad y por ello es necesario que previamente el afectado lo haya consentido o bien que exista previa autorización judicial⁵⁸.

C) Fase de obtención o confiscación de los datos.

La información contenida en el dispositivo electrónico se ha de incorporar al proceso como prueba electrónica de los elementos del delito investigado. Esto se puede llevar a cabo a través, bien de la aportación del propio sistema o equipo de almacenamiento (USB, DVD, disquete, etc) para que sea reproducido y examinado por el tribunal, bien con la aportación de una copia de la información⁵⁹ o a través de la práctica de un dictamen pericial para aquellos casos en los que sea necesario un análisis de la información por persona cualificada en la materia.

4.2.3. Diligencia de entrada y registro en lugar cerrado.

La Ley de Enjuiciamiento Criminal regula en su Título VIII (Artículos 545-588) los requisitos de la entrada y registro en lugar cerrado, la ocupación de libros y papeles y de la detención y apertura de la correspondencia escrita y telegráfica. Si conectamos dicho título con el contenido del artículo 18 de la Constitución, se pueden comprender las garantías exigidas para la diligencia de entrada y registro.

A) Fase de entrada y registro en el lugar cerrado.

Para la obtención de la prueba electrónica se deben respetar los derechos fundamentales, para garantizar la autenticidad del resultado de la diligencia se exigen una serie de garantías de legalidad ordinaria que se desarrollan a lo largo de los arts. 546 y ss. LECrim. Es necesario partir de la distinción entre la entrada y registro en lugar cerrado

⁵⁸ De Diego Díez, Luis Alfredo. *Control judicial sobre las piezas de convicción: la puesta a disposición judicial*. Diario la Ley, núm. 6196, Sección Doctrina, 23 de febrero de 2005 pág. 24.

⁵⁹ Se ha de tener en cuenta que únicamente han de ser ocupados los dispositivos que resulten estrictamente necesarios y se ha de realizar un volcado únicamente la a información relevante para el proceso (art. 574 LECrim).

que no sea domicilio de la entrada y registro en lugar cerrado como domicilio de una persona física o jurídica.

El primero de ellos, puede tratarse de cualquier lugar aislado o acotado respecto del exterior abierto pero que no sea constitutivo de domicilio. En este sentido, es necesario un auto de la autoridad judicial que esté conociendo o investigando un hecho con caracteres delictivos (art. 546 LECrim), también es necesaria la presencia del interesado (art.569 LECrim) así como la presencia en el acto del Secretario Judicial⁶⁰.

Para el caso que se haya realizado con todos los requisitos de la LECrim y haya sido autorizada previamente por el Juez, la prueba adquiere valor de prueba preconstituida y puede enervar la presunción de inocencia siempre que sea leída en el acto del juicio conforme a lo dispuesto en el art. 730 LECrim.

El segundo de ellos, trata de la diligencia de entrada y registro realizada en el domicilio de una persona física o jurídica. En este caso si se lleva a cabo sin autorización judicial previa o si no se cumplen todos los requisitos de motivación y proporcionalidad, se produciría una vulneración del derecho fundamental a la inviolabilidad del domicilio consagrado en el art. 18.2 CE por lo que esa prueba carecería de toda eficacia probatoria, deviniendo nula en aplicación del art. 11.1 LOPJ⁶¹.

Debemos tener en cuenta que antes de realizar un entrada y registro en el domicilio para la incautación de los equipos electrónicos los investigadores deben seguir una metodología, y si bien no existen estándares legales establecidos respecto a la informática forense hay muchas organizaciones trabajan en esto⁶². Actualmente se sigue la norma ISO 27037⁶³ la cual cuenta con una serie de principios:

- **Principio de aplicación de métodos.** Implica que la evidencia digital o electrónica debe adquirirse de la forma menos intrusiva posible, con el objetivo de preservar la originalidad de la prueba y en la medida de lo posible obteniendo copias de respaldo.

⁶⁰ Se trata de un concepto amplio tal y como expone Díaz Cabiale, José Antonio. (1992). *La admisión y práctica de la prueba en el proceso penal*. Madrid: editado por el CGPJ. Pág.157.

⁶¹ Vegas Torres, Jaime. (1996). *Prueba ilícita en particular (II): la ilicitud de la entrada y registro en lugar cerrado y sus consecuencias*. Cuadernos de Derecho Judicial. Madrid: editado por el Consejo General del Poder Judicial y la Escuela Judicial. Págs. 362-365.

⁶² Martín García, Pedro. (2000). *La prueba en el proceso penal*. Valencia: ed. Revista General de Derecho. Pág. 309.

⁶³ La norma ISO 27037 está orientada al procedimiento que deben seguir los investigadores en el escenario de la recogida, identificación y secuestro de la evidencia digital.

- **Principio de proceso auditable.** Debe seguirse un control sobre las actuaciones realizadas y los resultados obtenidos. Por tanto, el procedimiento que se haya seguido y la documentación generada deben haber sido validados y contrastados por las buenas prácticas profesionales.
- **Principio de proceso reproducible.** Tanto el método seguido como el procedimiento llevado a cabo deben poder ser reproducibles, verificables y argumentables, de forma que puedan ser comprendidos por los especialistas en la materia, quienes puedan dar validez y respaldo a las actuaciones realizadas.
- **Principio de proceso defendible.** Todos los elementos y herramientas utilizadas durante las actuaciones deben mencionarse de forma explícita, además de ser validadas y contrastadas en su uso para el fin para el cual se utilizan.

Dependiendo del tipo de dispositivo, y de acuerdo con la ya mencionada norma ISO 27037, la actuación realizada se puede dividir en tres fases:

1. **La identificación.** Es necesario localizar e identificar las potenciales informaciones o elementos de prueba en sus dos posibles estados, el físico y el lógico según sea el caso de cada evidencia.
2. **La recolección y/o adquisición.** Se trata de incautar los dispositivos y la documentación que puedan contener la evidencia que se desea recopilar o bien la adquisición y copia de la información existente en los dispositivos.
3. **La conservación/preservación.** La evidencia digital o electrónica ha de ser preservada para garantizar su posterior utilidad, por lo que las acciones de este proceso están claramente dirigidas a conservar la cadena de custodia, la integridad y la originalidad de la prueba

B) Fase de acceso a la información contenida en su interior.

En el momento que los agentes autorizados judicialmente intervienen para registrar las dependencias y pertinencias que en lugar se encuentren, también se incluye el registro de los dispositivos electrónicos que se presume puedan contener evidencias de la comisión del delito que esté siendo investigado⁶⁴. Además cabe resaltar, como la jurisprudencia ha venido haciendo, la necesaria autorización judicial para ampliar el

⁶⁴ Sánchez Núñez, Teresa. (2007). *Jurisprudencia del Tribunal Constitucional sobre el uso de las nuevas tecnologías en la investigación penal*. Cuadernos de Derecho Judicial. Madrid: editado por el Consejo General del Poder Judicial. Pág. 271.

registro a los denominados hallazgos casuales, es decir, aquellos objetos o instrumentos de otras infracciones penales que no son objeto del proceso⁶⁵.

Si bien es necesario mencionar que para el caso que se tenga constancia de que las pruebas del delito se encuentran en dispositivos electrónicos localizados en un local cerrado sería más adecuado que el auto de entrada y registro autorizase también el registro de dichos dispositivos⁶⁶.

C) Fase de obtención o confiscación de los datos.

Durante la práctica del registro puede ser objeto de aprehensión el propio dispositivo electrónico y sus elementos accesorios o únicamente los datos o informaciones relevantes para el proceso a través de la copia y volcado de los mismos.

4.2.4. Registros de información accesible y registros remotos.

Se trata del registro de información accesible, sin necesidad de proceder a la aprehensión física. Se debe diferenciar entre el registro tradicional: aquel acceso a los datos contenidos en el propio sistema informático o en el equipo de almacenamiento, y el registro remoto: aquel acceso a los datos existentes en otro sistema de información accesible desde el primero o disponible para éste.

En cuanto al registro remoto, éste es un tipo de registro muy útil en aquellos casos que es necesaria una actuación ágil y rápida como en casos en los que el acceso al lugar donde se halla supone un peligro para la vida o integridad física de los agentes o de la propia información o cuando el dispositivo electrónico es por ejemplo un Smartphone que está en constante movimiento⁶⁷.

La técnica utilizada consiste en acceder, mediante la previa instalación en el sistema investigado, de un software que permita a los investigadores escanear ya sea el disco duro o el resto de unidades de almacenamiento para remitir de forma remota y automatizada su contenido al técnico informático responsable de la investigación.

⁶⁵ Tal y como apunta la STS núm. 785/2008, de 25 noviembre, F.J. 2º (RJ 2009\556).

⁶⁶ Así lo entiende Castillejo Manzanares, Raquel. (2010) *Medios Probatorios. Hacia un nuevo proceso penal. Cambios necesarios*". Madrid: ed. La Ley, pág. 125 y ss.

⁶⁷ Ortiz Pradillo, Juan Carlos (2008). *Nuevas medidas tecnológicas de investigación criminal para la obtención de la prueba electrónica*. Madrid: ed. La Ley, pág. 276.

Los registros remotos sobre equipos informáticos están regulados en los arts. 350 y ss. Del PLECRim.- 2013, donde se exige la previa autorización judicial y se concretan los requisitos de tal autorización judicial.

Puesto que este tipo de registro supone una injerencia en derechos fundamentales como son el derecho a la intimidad, el secreto de las comunicaciones y en algunos casos, el derecho a la autodeterminación informativa, es necesario un pleno sometimiento a los criterios que la jurisprudencia ha desarrollado en el ámbito de los sistemas de información y de las telecomunicaciones. En este sentido, se exige a las autoridades del sistema penal un especial rigor tanto en la concurrencia de los presupuestos habilitantes ligados al principio de proporcionalidad como al control jurisdiccional de su ejecución⁶⁸.

Por otro lado, dentro de lo que se puede denominar registro tradicional, para el caso que se realizara una entrada y registro en lugar cerrado y se pudiera conocer de las pesquisas realizadas, que existe parte de información en otro sistema informático el cual es disponible o se puede acceder desde el primero, los investigadores deberán solicitar autorización judicial para ampliar el registro al otro sistema accesible desde el primero de conformidad con el art. 350.3 PLECRim.-2013⁶⁹.

Es una deslocalización de la información la cual se almacena de manera permanente en servidores que se alojan en cualquier parte del mundo y se envía a través de Internet a cachés temporales del equipo informático del usuario como pueden ser tabletas o Smartphone⁷⁰.

Del mismo modo, para el caso que se realizara una entrada y registro fuera de lugar cerrado, los agentes investigadores deberán solicitar autorización judicial para registrar el contenido de los datos e información que se hallen en otro sistema accesible desde el primero.

⁶⁸ STC núm. 173/2011 de 7 noviembre, F.J. 4º (RTC 2011\173).

⁶⁹ En este sentido, el art. 19.2 del Convenio de Budapest establece que “el ordenamiento ha de contemplar la posibilidad de que las autoridades competentes procedan a ampliar rápidamente el registro o forma de acceso similar al otro sistema”.

⁷⁰ Ortiz Pradillo, Juan Carlos. Ob. Cit. Pág. 289.

4.2.5. Registros transfronterizos.

Se trata del supuesto de registro de información accesible o registro remoto en el que los datos se hallan almacenados en un sistema informático o servidor situado fuera del territorio nacional.

El art. 32 del Convenio de Budapest⁷¹ establece que únicamente en los casos en los que conste consentimiento lícito y voluntario de la persona legalmente autorizada para revelar los datos y en el caso que se trate de datos informáticos almacenados que se encuentren a disposición del público, es decir, en una fuente abierta, la autoridad investigadora podrá acceder a los datos e información que se encuentren almacenados fuera de su jurisdicción nacional.

En el art. 31 del Convenio, se establece que en el resto de supuestos será necesario vehicular la acción investigadora a través de la cooperación judicial internacional. Ello implica que se deberá remitir la correspondiente solicitud de asistencia judicial internacional fundamentándose en el propio Convenio de Budapest o en otro instrumento internacional que pueda resultar de aplicación⁷².

En la Unión Europea, existe la posibilidad de solicitar la retención de los datos afectados y de forma posterior pedir la entrega o transmisión de dichos datos al amparo del instrumento internacional que cubra dicha actuación, ofreciendo así más agilidad a la asistencia judicial⁷³.

⁷¹ Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. Ratificación publicada en: BOE núm. 226, de 17 de septiembre de 2010, páginas 78847 a 78896.

⁷² Dependiendo del caso podrán ser aplicables, entre otros, el Convenio de 29 de mayo de 2000 relativo a la asistencia judicial en materia penal entre Estados miembros de la UE, el Convenio relativo al blanqueo, seguimiento, embargo y decomiso de los productos del delito de 8 de noviembre de 1990, el Convenio de ONU contra el tráfico ilícito de estupefacientes y sustancias psicotrópicas de 20 de diciembre de 1988, o el Convenio de ONU contra la delincuencia organizada transnacional, firmado en Palermo el 13 de diciembre de 2000.

⁷³ Esta posibilidad se encuentra regulada en la Ley 18/2006, la cual desarrolla la orden europea de embargo o aseguramiento de prueba regulada por Decisión Marco de 22 de julio de 2003.

4.3. Durante el juicio oral.

4.3.1. Procedimiento probatorio.

a) Proposición

En el proceso penal existe la posibilidad de la prueba practicada de oficio, con carácter general serán las partes las que propongan prueba en sus escritos de calificación provisional (art.656 LECrim) o de acusación y defensa (art. 781.1, 784.1 y 2 LECrim) o bien en el mismo trámite del juicio (art. 969 LECrim) según se trata de proceso ordinario, abreviado o juicio de faltas respectivamente⁷⁴.

b) Admisión

Es el acto por el que el Juez determina los medios de prueba que deben practicarse mediante un auto que deberá fundarse en la observancia de los requisitos exigidos, bien con carácter específico para cada medio de prueba en concreto o bien con carácter general. Sólo pueden admitirse los medios de prueba previstos legalmente, que provengan de una fuente lícita y que sean pertinentes y útiles.

c) Práctica

Teniendo en cuenta que existen normas específicas para los diferentes medios de prueba, en general, la prueba se practica en el local del órgano jurisdiccional (excepcionalmente puede que deba practicarse en otro lugar), siguiendo el orden estipulado en su proposición por las partes en las calificaciones, (si bien puede alterarse) y se practicarán en el juicio oral (si bien existe la posibilidad de la anticipación de la prueba).

4.3.2. El juicio oral

Si a la primera fase la hemos denominado “procedimiento preliminar” a ésta habría que llamarla “procedimiento principal” si bien es aconsejable seguir a la terminología de la LECrim y hablar de juicio oral. La fase del juicio oral se inicia con el auto de apertura del juicio oral y termina con la declaración formal de conclusión de la vista, previa a la

⁷⁴ Es necesario resaltar que esta regla general tiene excepciones respecto a la práctica de careos, pruebas de oficio, aparición de nuevos hechos o pruebas o al cambio de tipificación penal todo ello previsto en los arts. 729, 746.6, 730, 786.2 y 788.4 LECrim.

sentencia. Entre estos actos se incardinan otros muchos, entre los cuales el que aquí nos interesa es el de la vista o el juicio oral en sentido estricto.

Dentro del juicio oral tiene lugar el debate jurídico, compuesto por una o más sesiones en las cuales se van a practicar las pruebas admitidas⁷⁵.

Vamos a ver de qué forma, a través de qué cauce la prueba electrónica puede incorporarse en el proceso de entre las formas aceptadas legalmente⁷⁶.

4.3.2.1. Como prueba pericial:

En aquellos casos en los que se precisan conocimientos informáticos específicos, la prueba electrónica puede consistir en una pericial autónoma, no supeditada a otros medios, como por ejemplo para el caso que se precise averiguar el número de visitas recibidas por una página web. Por otro lado, también puede tener un papel no autónomo sino instrumental, cuando tanto para percibirla como para valorarla precisa de una pericial informática auxiliar, por ejemplo, cuando se quiere probar que una firma corresponde a una persona en concreto⁷⁷.

La tipología de pericias a realizar sobre los elementos ocupados depende de las necesidades probatorias de los hechos investigados, por lo que pueden ser pericias de autenticidad, pericias de contenido, de funcionamiento, de recuperación de datos o sobre Internet, entre otras.

A) Actos previos

La prueba pericial informática va precedida de una investigación pericial por lo que antes de incorporar el dictamen pericial informático como medio de prueba en el juicio oral, es necesario obtener la materia objeto de pericia y realizar la pericia informática así como emitir el dictamen acompañándolo de las conclusiones del perito especializado.

Es necesario que los archivos hayan mantenido una cadena de custodia, por lo que el perito está obligado a especificar en su informe los pasos seguidos desde que se

⁷⁵ Montero Aroca...*Derecho Jurisdiccional III...Ob.Cit.* Págs. 228- 229.

⁷⁶ Sanchís Crespo, Carolina. (1999). *La prueba por soportes informáticos*. Valencia: ed. Tirant lo Blanch. Pág. 99.

⁷⁷ Abel Lluch, Xavier; Picó i Junoy, Joan; Richard González, Manuel (dir). (2011). *La prueba judicial. Desafíos en las jurisdicciones civil, penal, laboral y contencioso-administrativa*. Madrid, Ed. La Ley. Pág. 360.

intervienen o reciben los equipos informáticos hasta que se presenten los archivos relevantes⁷⁸. No pueden alterarse los soportes, elementos informáticos originales por lo que se obliga a trabajar con copias clónicas. Se debe garantizar que el material incautado pueda ser examinado en su identidad e integridad, es decir, no puede existir duda alguna acerca de que lo examinado no sea exactamente lo ocupado en la actuación⁷⁹.

Respecto al informe pericial, éste debe comprender dentro de lo posible: la descripción del objeto en el estado o modo que se halle, la relación detallada de todas las operaciones practicadas por los peritos y su resultado, las conclusiones a las que llegan después de examinar los datos los peritos de conformidad con los principios y reglas de su especialidad.

B) Conversión de la fuente de prueba en medio de prueba.

Respecto a la incorporación del dictamen pericial informático como medio de prueba en el juicio oral será de aplicación la regulación de la prueba pericial (arts. 656 y ss LECrim) pero singularizada en atención a los factores subjetivos, objetivos y derivados de su propia especificidad.

Puesto que los dispositivos electrónicos no mantienen una relación unívoca con un solo medio de prueba, las informaciones que contienen pueden incorporarse al proceso a través de diferentes medios de prueba, así por ejemplo si se trata de sonidos podrán ser transcritos, si se trata de imágenes podrá decantarse por imprimirlas también en papel, o podrán apreciarse las imágenes en pantalla ante el Juez abriendo los archivos respectivos, etc⁸⁰.

La norma general es que la prueba pericial se practique en la vista del juicio oral, presidida por los principios de oralidad, publicidad, contradicción e inmediación. Al tratarse de una prueba electrónica, con las dificultades que la temática conlleva, en muchos supuestos será necesario un personal técnico que clarifique o ayude a comprender el significado de su contenido complejo, por lo que se hará imprescindible

⁷⁸ Es necesario tener presente que el objeto del peritaje es presentar el contenido sólo de los archivos que puedan tener relevancia jurídica, informando de su significado y características.

⁷⁹ Como es el caso de la SAP de Barcelona núm. 95/2008, de 29 enero, (ARP 2008\317).

⁸⁰ Pasamar, A. (2006). *Empresa y prueba informática en el libro del mismo título "Empresa y Prueba informática"*. Colección de formación continua de la Facultad de Derecho ESADE. Barcelona: ed. URL, J.M. Bosch. Pág. 24 y ss.

el apoyo externo en cuanto a la comprensión de los datos o incluso a la mera conexión o ejecución del programa que los contenga.

Pese a ello, es posible que se practique como prueba anticipada a propuesta de las partes en sus escritos de conclusiones, en caso de que se temiera que no va a poder practicarse en el juicio oral o si pudiera motivar su suspensión.

En relación con la exhibición en el acto de la vista del juicio oral del material o soporte informático que contenga la información y datos sobre los que verse un determinado análisis pericial previamente incorporado a los autos durante el período de instrucción, la jurisprudencia, de forma excepcional no ha privado de valor y eficacia al referido informe pericial ya incorporado y que cuyo objeto de análisis era un soporte electrónico que no se ha examinado en plenario. Admitiendo así “la inexistencia de indefensión por falta de examen en el plenario de la pieza de convicción interesada, desestimando el motivo planteado por las defensas⁸¹”.

La jurisprudencia ha convertido el dictamen pericial en prueba preconstituida documental, perfectamente evaluable en sentencia sin ratificación en la vista del juicio oral⁸². De igual forma se ha invertido la carga de su impugnación, obligando a quien lo cuestione a expresar en su escrito de conclusiones los motivos concretos de su discrepancia para permitir el sometimiento final al perito a contradicción en la vista del juicio oral⁸³.

4.3.2.2. Como prueba testifical:

La prueba testifical consiste en intentar obtener de terceros ajenos al proceso datos que puedan ayudar al sentenciador a formar su convicción sobre los hechos y responsabilidades que se deducen de ellos⁸⁴.

Así, el contenido de una prueba electrónica, como puede ser un e-mail puede ser enseñado a testigos o a las partes con el objetivo de ayudar al Juez o Tribunal a formar su convicción después de oír sus explicaciones. Ocurre lo mismo que ocurriría si se exhibiese un dibujo de un accidente de tráfico y se hicieran preguntas entorno al mismo,

⁸¹ STC núm. 480/2009, de 22 mayo, F.J. 1º y 2º (RJ 2010\662).

⁸² STC núm. 128/1990 de 5 julio (RTC 1990\128).

⁸³ STC núm. 1305/2006, de 27 diciembre (RJ 2007\501).

⁸⁴ Montero Aroca, Juan; Gómez Colomer José Luis; Montón Redondo, Alberto; Barona Vilar, Silvia. “Derecho Jurisdiccional III, proceso penal” 21ª edición. Valencia, Ed. Tirant lo Blanch, 2013, pág.119.

lo único que cambia son las características de prueba al tratarse de un soporte electrónico.

El interrogatorio de testigos se valora conforme a las reglas de la sana crítica, atendiendo a la razón de ciencia que ofrezca el testigo, sus circunstancias personales. Un testigo puede ayudar a dar nitidez a una teoría si puede afirmar o desmentir que un determinado sujeto a enviado un SMS, identificando su destinatario, su contenido o forma de expresión, porque todas las operaciones se efectuaron con su presencia⁸⁵.

4.3.2.3. Como reconocimiento judicial:

El reconocimiento judicial es la percepción de forma directa por parte del Juez de los hechos que son objeto de prueba. A diferencia del resto de medios de prueba, en el reconocimiento judicial nada se interpone entre el juzgador y el hecho⁸⁶.

Cuando acudimos a la Ley de Enjuiciamiento Criminal las únicas referencias que encontramos respecto al reconocimiento judicial como prueba son: por un lado, el reconocimiento judicial de la identidad de la persona acusada (arts. 368 y 369) y, por otro lado, regula como prueba la inspección ocular (arts. 326, 327 y 727).

Parte de la doctrina⁸⁷ resalta la reticencia a la práctica de esta prueba en el ámbito penal, no ya solo en cuanto a la ineficacia de sus resultados, sino en orden a llevarse a efecto en el acto de la vista oral por estimarse inútil dado el tiempo transcurrido y poder, además, vulnerar los principios de concentración y publicidad. Razones por las que se aconseja su restricción a situaciones en que nos e disponga de ningún otro medio para determinar los hechos.

Debemos señalar la importancia de la escasa regulación contenida en la LECrim, la cual no tiene en cuenta la existencia de las nuevas tecnologías y en consecuencia tampoco de los nuevos soportes electrónicos ni de su obtención, incorporación y valoración como pruebas electrónicas o digitales en el proceso penal. Si bien es lógico pensar que el reconocimiento judicial puede ser un medio idóneo para la percepción de evidencia digital, pues el examen directo por un Juez del contenido de, por ejemplo,

⁸⁵ Abel Lluch, Xavier; Picó Junoy, Joan. (dir). (2008). *Colección de Formación Continua de la Facultad de Derecho de ESADE*. Serie Estudios Prácticos sobre los medios de prueba, núm. 2. Barcelona: ed. J. M. Bosch. Págs. 49 a 55.

⁸⁶ Abel Lluch, Xavier. (2012). *Derecho probatorio...Ob.Cit.*Pág. 1033.

⁸⁷ Como lo es la opinión dada por Alberto Montón Redondo, Alberto. (2013). *Derecho Jurisdiccional III, proceso penal*. (21ª edición). Valencia: Ed. Tirant lo Blanch. Pág.316.

una página web o de un e-mail puede resultar muy útil para la formación de la convicción judicial resultando un elemento probatorio decisivo.

De conformidad con lo dispuesto en art. 4 CC la legislación civil será de aplicación analógica en lo no previsto por las leyes penales, de modo que si acudimos a la Ley de Enjuiciamiento Civil en sus artículos 353 y siguientes se establecen los extremos legales que deben cumplirse para el reconocimiento judicial o cibernavegación.

Mientras que en el art. 227 LECrim se habla de inspección ocular, el artículo 353 LEC tiene una regulación más abierta, dando cabida no sólo a que el Juez deba percibir con la vista (inspección ocular) sino que puede percibir con cualquiera de sus sentidos la prueba⁸⁸.

Siendo una prueba directa, lo esencial es que el juez perciba directamente el entorno informático, sea tecleando personalmente el ordenador, o sea visionando la pantalla y el entorno digital a partir de las instrucciones de un técnico. El objeto de reconocimiento puede ser un lugar, entendiéndolo como lugar virtual, o puede ser un objeto, por ejemplo, un ordenador a través del cual se accede a la red.

La práctica del reconocimiento judicial precisa una referencia al lugar, tiempo, forma y la eventual concurrencia con otros medios de prueba. Así, existe la posibilidad que pueda practicarse, de oficio o a instancia de parte, el reconocimiento judicial junto con la prueba pericial (art. 356 LEC) caso en el que se procederá a la navegación por la red o la percepción de la pantalla del ordenador y de forma simultánea a la aportación de la experiencia específica técnica por parte del perito. También es posible que pueda practicarse de forma conjunta con el interrogatorio de las partes y testigos, caso en el cual se practicaran las pruebas de forma sucesiva, primero el reconocimiento por parte del Juez y acto seguido la declaración de la parte o del testigo⁸⁹.

⁸⁸ En este sentido la literalidad del art. 535 establece “el reconocimiento judicial se acordará cuando para el esclarecimiento y apreciación de los hechos sea necesario o conveniente que el tribunal examine por sí mismo algún objeto, lugar o persona” sin hacer expresa referencia a la forma de apreciar ese examen.

⁸⁹ Abel Lluch, Xavier; Picó i Junoy, Joan; Richard González, Manuel (dir). (2011). *La prueba judicial. Desafíos en las jurisdicciones civil, penal, laboral y contencioso-administrativa*. Madrid: ed. La Ley. Pág. 366.

4.3.2.4. Como prueba documental:

La prueba electrónica también puede ser incorporada como documento electrónico, solo es necesario pensar en un e-mail, el cual no deja de ser un documento aunque con la singularidad de que aparece recogido en un soporte informático.

El art. 26 del CP proporciona una definición legal de documento: "A los efectos de este Código se considera documento todo soporte material (presente o futuro) que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica".

Cabe decir que el CP prevé determinadas clases de documentos típicos que son los electrónicos, públicos, oficiales, mercantiles, privados y secretos. Estas clases son las que tienen relevancia a efectos penales. El concepto penal de documento tiene cabida a efectos probatorios, pero la definición del art. 26 del CP está limitada a los efectos del propio Código. Dicha definición es aplicable a delitos de daños documentales, de falsedades documentales, de infidelidad en la custodia de documentos, de obstrucción a la justicia y deslealtad profesional, así como relativos a la defensa nacional.

El Tribunal Supremo en distintas ocasiones ha establecido como requisitos para que el documento pueda constituir prueba: ⁹⁰ su constancia en soporte indeleble, es decir imborrable, su procedencia humana, entendiéndose que el autor debe ser determinable por el propio documento, la declaración debe ser significativa en sí misma, por lo que no caben escritos encriptados u otros análogos, deben encontrarse en el tráfico jurídico y debe ser original, por lo que no tienen cabida las fotocopias o copias⁹¹.

Como ya se ha venido subrayando a lo largo del presente trabajo, el desarrollo de las nuevas tecnologías ha propiciado la aparición de delitos electrónicos así como la utilización de soportes electrónicos como pruebas. La consecuente necesidad de probar se encuentra carente de regulación específica en nuestro derecho positivo y ello ha

⁹⁰ STS núm. 1234/1998, de 22 octubre, F.J. 2º (RJ 1998\8716), STS núm. 346/1999, de 3 marzo, F.J. 1º t 2º (RJ 1999\2091).

⁹¹ STS núm. 1464/2002 de 13 septiembre, F.J. 2º. (RJ 2002\8443) .

llevado a su incardinación en el ámbito de prueba documental, dada la amplitud legal del concepto documento⁹².

De acuerdo con la jurisprudencia, por documento no debe entenderse estrictamente toda representación gráfica del pensamiento plasmada por escrito, sino cualquier instrumento mueble apto para la incorporación de señales expresivas de aquel y que lo reproduce más o menos fidedignamente⁹³.

Si atendemos a la casuística, la jurisprudencia ha establecido expresamente algunos de los documentos que pueden ser incorporados al proceso como prueba digital como son los mensajes de correo electrónico⁹⁴ o el soporte informático en el que se fija la disponibilidad de una tarjeta de crédito⁹⁵.

Por su parte, la Consulta de la Fiscalía General del Estado de 10 de mayo de 2001 considera documento a efectos penales la tarjeta de prepago utilizada en cabinas públicas de teléfono⁹⁶.

4.3.2.5. Como reproducción de palabras, sonidos e imágenes.

Si bien es cierto que en el ámbito penal no existe referencia expresa alguna sobre su consideración como medio de prueba⁹⁷, esa ausencia no impide su tratamiento como tal.

De acuerdo con la jurisprudencia, ello se explica porque en el proceso penal, al igual que en el civil, no rige un sistema de “*numerus clausus*”. La regulación de la LECrim es insuficiente, con remisiones continuas a la regulación de cada medio al correspondiente acto de investigación sumarial, así como la falta de previsión de problemas derivados de los modernos medios de prueba, que no obstante, son reconducibles al concepto actual de “documento” en sentido amplio. Sentido que integra, siguiendo al art. 299.2 LEC, los medios de reproducción de palabra, sonido e imagen así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, etc⁹⁸.

⁹² Montero Aroca, Juan; Gómez Colomer José Luis; Montón Redondo, Alberto; Barona Vilar, Silvia.(2013). *Derecho Jurisdiccional III, proceso penal*. (21ª edición). Valencia: Ed. Tirant lo Blanch. Págs.315-316.

⁹³ STC núm. 190/1992, de 16 noviembre, F.J. 2º (RTC 1992\190).

⁹⁴ SAP de Valencia núm. 127/2001, de 24 mayo, F.J. 3º (ARP 2001\589).

⁹⁵ SAP de Tarragona núm. 457/1998, de 1 septiembre, (ARP 1998\3818).

⁹⁶ Si bien la SAP de Madrid, de 23 noviembre 2000, F.J. 2º (AC 2002\136) entiende que la tarjeta prepago imitada empleada en una cabina telefónica no es documento a efectos penales.

⁹⁷ A excepción de la prevención del art. 726 LECrim.

⁹⁸ SAP de Tarragona núm. 220/2013, de 29 mayo, F.J. 1º (JUR 2013\272852).

Las partes pueden proponer como medio de prueba la reproducción ante el tribunal de palabras, imágenes y sonidos captados mediante instrumentos de filmación, grabación u otros semejantes. Las palabras, imágenes y sonidos deben constar registrados en los soportes técnicos correspondientes los cuales, como regla general, habrán de haber sido aportados al proceso por las partes, como si de documentos se tratase⁹⁹.

Por tanto, pueden aportarse como fuentes de prueba cintas de vídeo, disquetes, memorias, etc. para su reproducción o conocimiento a través de los medios técnicos pertinentes. Además, podrán acompañar si lo estiman pertinente, su transcripción escrita, dictámenes como la prueba testifical del a persona responsable de la grabación y filmación o dictámenes periciales acerca de su autenticidad y exactitud, entre otros.

Si bien es cierto, que debe prestarse especial atención a los supuestos en los que dichas filmaciones o grabaciones puedan vulnerar derechos fundamentales como son el secreto de las comunicaciones y a la intimidad¹⁰⁰.

⁹⁹ STS núm. 1067/1992, de 30 noviembre, F.J.1º. (RJ 1992\9458) sobre su introducción como prueba documental.

¹⁰⁰ SAP de Córdoba núm. 136/2002, de 25 mayo, F.J. 2º (AC 2002\1000).

5. EFICACIA PROBATORIA DE LA PRUEBA ELECTRÓNICA

Esta modalidad de prueba presenta una serie de especialidades que hacen que su eficacia y su valoración tengan unas connotaciones distintas a las del resto de pruebas tradicionales.

Por un lado, la legislación al respecto es insuficiente y hace que se deba atender a reglas analógicas que proporcionan otras instituciones reguladas con más detalle, así como acudir a la jurisprudencia existente y estudiar el derecho comparado a fin de extraer criterios útiles que sirvan para ponderar y valorar las dificultades interpretativas que se presentan.

Todo ello implica la necesidad de una flexibilidad permanente para poder estar alerta sobre la última jurisprudencia nacional y extranjera a fin de conocer el tratamiento jurídico que se va otorgando a las innovaciones que van surgiendo.

Otro de los problemas que presenta la prueba electrónica es su complejidad para captar su funcionamiento, derivado de su contenido técnico-científico que conlleva la imprescindible búsqueda de asesoramiento experto, pericia informática para los casos de cierta dificultad o controversia.

Si bien el problema más extendido es el de la fiabilidad de la prueba electrónica por su fácil manipulación. Para poder realizar su valoración es necesario, tal y como ya se comentó, que supere el llamado “test de admisibilidad” cumpliendo con la integridad (el soporte no haya sido alterado ni manipulado), la autenticidad (constatación de la realidad del sujeto al que se atribuye y del contenido que refleja) y la licitud (obtención con respeto a los derechos y libertades fundamentales).

5.1. La valoración de la prueba electrónica.

La valoración de la prueba tiene como objeto establecer la conexión final entre los medios de prueba presentados y la verdad o falsedad de los enunciados sobre los hechos en litigio. La tarea valorativa es fundamental en cualquier proceso judicial y ha de ser llevada a cabo por el Juez o Tribunal que ha de resolver el caso, ya sea el órgano “ad quem” o, eventualmente, el Tribunal Supremo o el Tribunal Constitucional¹⁰¹.

¹⁰¹ Sanchís Crespo, Carolina. Ob.Cit. Pág. 121.

Puesto que valorar una prueba dentro de un proceso judicial no debe ser un acto arbitrario, parcial, injustificado, subjetivo ni antojadizo, la valoración de la prueba es una cuestión que se ha intentado, tanto legislativamente como a nivel doctrinal, regular de forma que no exista arbitrariedad en la apreciación de la misma por parte del Juez.

Por ello, se han venido expresando una serie de pautas valorativas que subrayan que las normas jurídicas “no son entidades que vagan sueltas por ahí” sino que se encuadran en “el mismo sistema jurídico”.

5.1.1. Prueba legal, prueba libre y sistemas mixtos de valoración.

En nuestro ordenamiento jurídico español se ha ido delineando, a lo largo del tiempo, un sistema de valoración legal primero, libre después y mixto actualmente. Lo esencial, según la jurisprudencia, es que tal sistema de valoración obedezca “a los dictados más estrictos de la lógica y de la semiótica” y a “principios de experiencia¹⁰²”.

A continuación, se analiza cómo son, respecto a la valoración de la prueba, cada uno de los distintos sistemas comentados:

Prueba legal. El recorrido comenzó por la ley, es decir, por el sistema de tarifa legal, formado en el siglo XIII y refinado y extendido en los siglos siguientes de los países del civil law.

Este sistema se basaba en la aplicación de reglas que establecían a priori y en términos generales el valor probatorio de algunos tipos de medios de prueba. Se basaba en largas y complejas listas de reglas detalladas que establecían el peso de cada medio de prueba específico. Por ello, el Juez veía reducida o incluso eliminada por completo la capacidad de valoraciones subjetivas o discrecionales, sólo tenía que sumar los valores de las pruebas positivas y negativas a cerca de cada hecho mediante una especie de cálculo algebraico¹⁰³.

Prueba libre. El método de libre valoración es aquel en el que el Juez deja de estar atado de forma rígida a lo que algunos autores llaman “cuadro piramidal de escalas probatorias”¹⁰⁴ y se le permite una mayor flexibilidad, si bien debe decidir teniendo en

¹⁰²Tal y como el Tribunal Supremo ha reiterado en sus sentencias: STS, de 6 de marzo de 1987 F.J. 2º,(RJ 1987\2454) y STS núm. 497/1998, de 3 abril, F.J. 3º (RJ 1998\3284).

¹⁰³ Taruffo, Michele. (2008). *La prueba*. Madrid: ed. Marcial Pons. Pág. 133-136.

¹⁰⁴ Así lo entiende Cabañas García, Juan Carlos. (1993). *La valoración de las pruebas y su control en el proceso civil*. Madrid: ed. Trivium. Pág. 50 y ss.

cuenta ciertos límites como son la racionalidad, la inmediación de la prueba o la necesidad de motivar su decisión.

En este sentido lo fundamental es que la decisión adoptada no carezca de la indispensable consistencia, que no exista quiebra del nexo causal que de forma lógica ha de llevar a la conclusión judicial y que, por tanto, no asalten dudas razonables. Además, en el momento de aplicar y valorar la norma que disciplina la prueba, se deben tener en cuenta las relaciones de interdependencia que nuestro sistema jurídico mantiene con la sociedad, por lo que se requiere una ponderación de aspectos como son los culturales, políticos, económicos, etc.

De todo lo descrito, no debe interpretarse que la “libre valoración” implique libertad sin límites ni ataduras legales, sino que se hace depender de criterios de valoración racional, es decir, se debe observar una metodología racional justificativa de la decisión adquirida y que debe expresarse de forma explícita en la misma.

En una sociedad como la nuestra, democrática, la decisión adoptada ha de ser objeto de control, incluso por el tribunal de casación puesto que nada le impide examinar si el razonamiento probatorio es lógico y suficiente o, por el contrario, no lo es.

La jurisprudencia ha entendido que el control a través de la casación incluye la posibilidad de verificar la racionalidad de las conclusiones obtenidas por el tribunal de instancia, explicitadas a través de la motivación, pudiendo rechazar la credibilidad que le concedió el tribunal sentenciador si sus conclusiones son contrarias a las máximas de la experiencia o incurren en arbitrariedad¹⁰⁵.

Sistema mixto de valoración. En el sistema español, el principio de libre valoración de la prueba es general porque atañe a cualquier medio de prueba cuyo valor no esté jurídicamente determinado de forma expresa, por lo que en realidad no se aplica en todos los casos. Algunos ejemplos son las reglas que prevén un valor probatorio legal de los documentos públicos y privados, o también de confesiones y juramentos.

La problemática que surge es que las normas reguladoras de la prueba no agotan el tema puesto que interpretar una prueba es una tarea compleja y su plasmación se realiza a base de argumentos. En nuestro ordenamiento jurídico los arts. 209 LEC y 741 LECrim establecen las reglas en la materia.

¹⁰⁵ STS núm. 90/2007, de 23 enero, F.J. 3º (RJ 2007\625).

Mientras que en la ley procesal civil se hace referencia a que en las sentencias deben expresarse “las razones y fundamentos legales del fallo”, en la ley reguladora del proceso penal, se hace una referencia al sistema de libre valoración, puesto que de forma expresa se indica que la sentencia se dictará “apreciando (el Tribunal) según su conciencia” las pruebas practicadas y lo manifestado por las partes procesales.

De ahí, se adelanta, que la clave de la valoración sea la expresión de su motivación, la cual deberá moverse entre la probabilidad y la certeza jurídica, tras aplicar reglas de experiencia y ejercer una “sana crítica” de los medios de prueba aportados en cada proceso.

5.1.2. Las reglas de la sana crítica, las máximas de experiencia y la certidumbre razonable.

Tal y como se ha descrito en el apartado anterior, la forma habitual de afrontar el problema de cómo el juzgador debe determinar el valor probatorio de los medios de prueba suele remitir de un modo vago y general al sentido común, a la experiencia común, a lo razonable o la racionalidad, sin definir criterios más precisos y específicos¹⁰⁶. Por ello, es necesario puntualizar a qué se hace referencia cuando se habla de la sana crítica, de la experiencia común y de la certidumbre razonable.

A) Reglas de la sana crítica:

Se destaca la no vinculación del Juez a las reglas tasadas de prueba, que suelen ser insuficientes, para recordar que además existen lo “principios jurídicos” y “valores” art. 1 CE, que sitúan a las reglas de la sana crítica en un plano de individualización flexible del caso, en el que la opinión de los expertos y la propia experiencia del Juez, configuran un método que entrega, en última instancia a la lógica, oídas las partes, la interpretación de las pruebas¹⁰⁷.

Si bien las reglas de la sana crítica no se encuentran codificadas, de acuerdo con la doctrina “han de ser tenidas como las más elementales directrices de la lógica humana”. Su importancia revierte en que son especialmente útiles a la hora de valorar pruebas contradictorias o la prueba indiciaria, interpretar informes periciales contradictorios o

¹⁰⁶ Taruffo, Michele. (2010). *Simplemente la verdad...* Ob. Cit. Pág. 184.

¹⁰⁷ Cabañas García, Juan Carlos. Ob.Cit. Pág. 140.

indicios... En suma, tareas que demandan una libre, aunque motivada, valoración del Juez.

La doctrina define a la sana crítica como el buen arte de juzgar, que tiene por objetivo alcanzar y establecer, con expresión motivada, la certeza sobre la prueba que se produce en el proceso¹⁰⁸.

Se trata de una valoración racional de la prueba, como una especie de estándar jurídico, que ofrece soluciones flexibles al caso pero que no se originan en la inventiva personal ni en la caprichosa interpretación del juez. La expresión “sana crítica” se ha considerado sinónimo de “sana filosofía” o “crítica racional”. Así, por ejemplo, se trata de poder valorar datos como puedan ser la moralidad de un testigo, la relación del testimonio con el hecho, el grado de implicación con la otra parte, etc.

Puesto que no debe tratarse de una interpretación arbitraria por parte del Juez, se considera que la sana crítica comporta una serie de razonamientos que deben expresarse en forma de motivación. Así, deben contemplarse el principio de razón suficiente; ningún hecho puede ser verdadero o existente, y ninguna enunciación verdadera, sin que haya una razón suficiente para que sea así y no de otro modo, el principio de contradicción; una cosa no puede ser y no ser al mismo tiempo, el principio de identidad; una cosa sólo puede ser lo que es y no otra, y el principio del tercero excluido; entre dos proposiciones de las cuales una afirma y otra niega, una de ellas debe ser la verdadera¹⁰⁹.

B) Máximas de experiencia:

La jurisprudencia suele hacer referencia a las máximas de la experiencia en sus resoluciones. Se trata de generalizaciones basadas sobre un cierto número de experiencias precedentes, pues la experiencia hace notable lo que ocurre normalmente en casos análogos.

La experiencia está asociada al sentido común, el hombre medio actúa en base a la experiencia que le es conocida, acumulando datos, conocimientos, cultura, que relaciona y por los que toma unas determinadas decisiones.

¹⁰⁸ Barrios González, Boris. (2004). *Ideología de la prueba penal*. (2ª edición). Ed. Jurídica Ancon. Pág.113.

¹⁰⁹ Younes Jerez, Simón. (2001). *Credibilidad y certeza en la prueba judicial*. Madrid: Ed. Leyer. Pág. 175.

Por ello, resulta importante para el Juez, como encargado de interpretar la prueba, la experiencia que éste tiene para ayudar a realizar la tarea que le es encomendada de valorar hechos, situaciones y las pruebas aportadas.

Es importante no confundir la experiencia con el conocimiento científico o las leyes de la naturaleza, las cuales son verdades axiomáticas, sino que la experiencia es relativa, puede aproximarse a la verdad pero no tiene porqué ser así¹¹⁰.

C) Certidumbre razonable:

Si bien la prueba es un medio que se utiliza para establecer la verdad de un hecho, el juicio valorativo emitido por el Juez, discurre entre la probabilidad y la certeza jurídica, teniendo puntos de conexión con la verdad.

Se defiende una certeza que excluya toda duda fundada y razonable puesto que es lo necesario y justo para poder pronunciar una sentencia de forma adecuada. Esa certeza no es una convicción íntima válida del juzgador, sino que trata de excluir toda probabilidad de una solución contraria a la que se adopta.

Es un tema complejo puesto que, pese a lo dicho anteriormente, en el fondo no es algo objetivo: la verdad está en los hechos, mientras que la certeza está en las personas, en el grado de convicción alcanzado por el destinatario de la prueba que viene obligado a su valoración¹¹¹.

Certeza es ausencia de duda o dudas razonables y de peso, incompatibles con lo que se cree. Es por ello que no puede existir una hipótesis alternativa, puesto que implicaría la existencia de una duda razonable respecto de que otra postura pudiera ser la correcta. Así, a través de la sana crítica, del buen sentido, de la experiencia y de la capacidad lógica de razonar se puede llegar a una elección que resulta más probable en el caso, alcanzando una “certeza razonable”¹¹².

¹¹⁰ Younes Jerez, Simón. Ob. Cit. Pág. 184 a 191.

¹¹¹ Ferrer Beltrán, Jordi. (2007). Ob. Cit. Pág. 98-115.

¹¹² Younes Jerez, Simón. Ob. Cit. Pág. 35.

5.1.3. La exigencia jurídica de motivación.

Los Jueces y Magistrados restan obligados a motivar sus decisiones, sentencias, autos e incluso providencias cuando se estime conveniente¹¹³ Se trata de una de las garantías más importantes incluidas en el derecho a la tutela judicial efectiva (art. 24 CE). De forma concreta, en materia de prueba, en el proceso penal se exige un auto admitiendo o denegando la prueba¹¹⁴.

La motivación es la tarea de dar razones, explicar, justificar un acto o decisión. Se trata de motivar siguiendo los cánones de racionalidad que aseguran una justificación más completa, simple y lineal. En esa justificación, se encuentra el límite a la arbitrariedad y la legitimación del papel del Juez en la sociedad actual.

Los mayores defectos que pueden cometerse son la denominada “motivación aparente” en los casos en los que se hace referencia a normas o criterios generales valorativos pero no se realiza una tarea justificativa real¹¹⁵. La más grave sería el déficit motivador¹¹⁶, aquellos casos en los que no se plasma la valoración de concretos medios probatorios, así como el empleo de argumentos a favor y en contra sin resolver la aparente contradicción de un modo lógico y racional.

5.1.3.1. Exclusión de la prueba ilícita.

Se habla de prueba ilícita tanto si se produce una vulneración directa de una norma o principio constitucional, como si se trata de una irregularidad que causa indefensión efectiva. Ello es porque el nexo causal entre actividad probatoria y vulneración del derecho fundamental, no cuenta con una prueba válida en que fundar la decisión de fondo del proceso, ya que jurídicamente nos encontramos ante una prueba inexistente y que debe ser expulsada del procedimiento¹¹⁷.

La jurisprudencia lo ha definido como “una garantía constitucional negativa, que impide la valoración de la prueba ilícita, por lesionar el derecho al proceso con todas las

¹¹³ Tal y como se desprende de los art. 120.3CE y 248 LOPJ.

¹¹⁴ Art. 659 LECrim proceso ordinario y art. 785.1 LECrim para el abreviado.

¹¹⁵ Un ejemplo de ello es la STS núm. 285/2006, de 8 marzo, F.J. 2º (RJ 2006\1003) la cual entiende sobre la sentencia que se recurre que la sentencia que se pierde en vacías expresiones probatorias.

¹¹⁶ Como es el caso de la STS núm. 855/2006, de 12 septiembre, F.J. 2º (RJ 2006\6345) que entiende que sobre la sentencia recurrida existe un vacío de expresión de análisis.

¹¹⁷ Encontramos su fundamento jurídico en el art. 11.1 LOPJ, que sostiene que “no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentado los derechos o libertades fundamentales”.

garantías, no permitiéndose la condena en base a tal prueba, al conculcar el derecho a la presunción de inocencia¹¹⁸.

Si bien es cierto que se impone una concepción casuística de la prueba ilícita, detrás de ese casuismo, hay una base ética general porque en toda prueba ilícita hay un proceder contrario a derecho, en el amplio sentido de la expresión, esto es, una actuación que infringe normas, principios o valores del proceso propios del ordenamiento jurídico¹¹⁹.

5.1.3.2. Denegación motivada.

La inadmisión de la prueba debe tener una motivación adecuada, en la que se especifique las razones que han llevado a la decisión adoptada. La decisión judicial no puede ser una mera intuición, conclusión sin conexión lógica o totalmente libre, sino que ha de acomodarse a criterios de racionalidad.

Es necesario valorar y tener en cuenta los intereses generales a la hora de denegar una prueba, como es el derecho de defensa, el cual se traduce en el derecho a proponer los medios de prueba pertinentes y la necesidad de realizar el enjuiciamiento impidiendo su demora.

La forma en la que debe motivarse la denegación de una prueba es conforme a la Constitución. Es decir, con pautas de racionalidad extraídas de los principios y normas constitucionales, ya que de acuerdo con la jurisprudencia “la resolución denegatoria de una prueba es un juicio jurídicamente vinculado a las exigencias impuestas en la Constitución, fundamentalmente a través de su artículo 9.3¹²⁰”.

Su fundamentación debe responder a “una interpretación y aplicación del Derecho ajena a toda arbitrariedad.¹²¹ Por lo que en caso de existir un atisbo de arbitrariedad resultaría vulnerado el derecho de defensa “en aquellos supuestos en los que el rechazo de la

¹¹⁸ STC núm. 202/2001, de 15 octubre F.J.3º (RTC 2001\202).

¹¹⁹ Martí Mingarro, Luis. (2003). La prueba ilícita penal. (3ª edición). Navarra: ed. Aranzadi SA. Pág. 42-47.

¹²⁰ Así lo expone la STS núm. 669/2003, de 7 mayo, F.J. 4º (RJ 2003\5258) la cual cita a la STS de 2 de marzo de 1992(RJ 1992, 1677).

¹²¹ STC núm. 264/1988, de 22 diciembre. F.J. 2º y 3º (RTC 1988\264).

prueba propuesta, en tiempo y forma, carezca de toda motivación, o la motivación que se ofrezca pueda tacharse de manifiestamente arbitraria o irrazonable¹²²”.

5.1.3.3. Prohibición de toda indefensión.

La indefensión es aquella que impide o limita, de modo trascendente, la capacidad de alegación y prueba de una parte procesal. Es decir, la que afecta al derecho de contradicción, alterando el ejercicio de las reglas procesales, y en concreto, el derecho de igualdad de armas de las partes¹²³.

Debe tratarse de un daño que implique un perjuicio definitivo en los derechos e intereses sustantivos que defienda la parte afectada, un acto procesal que altere el sentido del fallo a costa de una parte. De acuerdo con la jurisprudencia, el perjuicio producido ha de ser algo real y efectivo, que se traduzca en un menoscabo auténtico o indefensión material, del derecho de defensa, y no en una mera expectativa potencial y abstracta que pueda verse frustrada¹²⁴.

Llevado a la temática probatoria, implica el impedimento de aportación de una prueba lícita o la admisión de una prueba ilícita, siempre que ello se deba a una falta atribuible al órgano judicial que, con ello, pierde la imparcialidad objetiva propia de su cargo. Por tanto, significa que si tal infracción es debida a una negligencia de la parte que no usa sus derechos, muestra desinterés, impericia, inactividad, negligencia, se aquieta a infracciones ajenas o coopera con la conducta dolosa o culposa de la otra parte, no operará la infracción del derecho a la defensa¹²⁵.

5.2. Criterios y especialidades valorativas aplicables a la prueba electrónica.

El mayor problema con que nos encontramos a la hora de señalar pautas de valoración concretas de la prueba electrónica o tecnológica, es la falta de una regulación específica sobre la misma. La inexistencia de tal normativa obliga a la aplicación analógica sobre la prueba, en general.

Aunque se parte del principio de libertad de presentación y evaluación de la prueba, el órgano juzgador debe no perder de vista una idea general: esa valoración “subjetiva” del

¹²² STC núm. 183/2002, de 14 octubre, F.J. 2º (RTC 2002\183).

¹²³ STC núm. 210/1999, de 29 noviembre, F.J. 2º (RTC 1999\210).

¹²⁴ STC núm. 88/1999 de 26 mayo, F.J. 2º y 3º (RTC 1999\88).

¹²⁵ STC núm. 68/1991, de 8 abril, F.J. 2º (RTC 1991\68).

Juez debe adecuarse a las innovaciones tecnológicas, respetando en todo caso las garantías constitucionales del debido proceso.

Por tanto, resulta de aplicación todo lo que se ha expuesto en los puntos anteriores si bien, de acuerdo con la jurisprudencia y la casuística se desprenden algunas especialidades en la valoración de la prueba electrónica que veremos a continuación.

5.2.1. Racionalidad.

El ya comentado régimen de libre valoración de la prueba que rige en nuestro sistema jurídico, no puede ser identificado con un subjetivismo arbitrario, dada la taxativa interdicción de la arbitrariedad postulada en el art. 9.3 CE y la exigencia de la motivación en las resoluciones judiciales, es decir, tal y como especifica la jurisprudencia tales resoluciones deben dar cuenta de la “historificación de los hechos en adecuado ensamblaje con ese acervo de mayor o menor amplitud, de datos acreditativos o reveladores, que haya sido posible concentrar en el proceso¹²⁶”.

Ello implica la necesaria existencia de una conexión lógica y racional entre la prueba y el hecho probado que el tamiz de la conciencia¹²⁷, se convierta en un ejercicio de racionalidad y sentido común, expresado en la resolución mediante los idóneos razonamientos que han llevado a la concreta decisión.

En la prueba electrónica, por sus características propias, existe una especialidad que no se puede encontrar en el resto de pruebas: el soporte en el que se encuentran. Este tipo de pruebas se contienen en soportes tales como disquetes, ordenadores, tarjetas de memoria, Smartphone, etc. Por tanto, existen dos elementos a analizar: uno técnico y externo llamado hardware y otro lógico e interno que recibe el nombre de software.

En cuanto al primero, hardware, es necesario comprobar las posibles incidencias en su etapa de elaboración, fabricación, funcionamiento o transmisión tales como fallos de los programas, humedad, disfunciones por temperaturas extremas, acumulación desordenada de información proveniente de distintas terminales de entrada, etc.

Mientras que respecto al segundo, el software, es necesario comprobar aspectos relativos a la averiguación de quién confeccionó el programa, si intervino persona no

¹²⁶ STS de 18 abril de 1988, F.J. 2º y 3º (RJ 1988\2801) .

¹²⁷ Al que se alude en el art. 741 de la LECrim.

autorizada, alguien diferente al que aparece como autor, si se empleó su clave por un tercero, etc.

La prueba contenida en soporte electrónico debe ser reproducida, tal y como se desprende del art. 730 LECrim, confiriendo a la voluntad de las partes del proceso, con la superior decisión del órgano juzgador, la decisión al respecto, ya que el conocimiento de la prueba contenida en soporte electrónico puede conducirse por diversas vías (a través de su lectura, imprimiendo los datos, reproduciéndolo en pantalla, etc) pero siempre ha de asegurarse que el órgano juzgador tenga acceso y se entere de tal contenido para poder valorar el material que le ha de informar para tomar su decisión.

Es en este punto en el que los Jueces deben dar un paso más con respecto al resto de pruebas, por tener las electrónicas unas características inherentes, el órgano juzgador debe motivar su resolución a través de lo que algunos autores han calificado como “sana crítica especialísima”¹²⁸ entendiendo que no sólo deben basarse en la lógica y sentido común del hombre medio, sino que deben de pasar a un nivel superior que es el que requieren las nuevas tecnologías, haciendo un esfuerzo añadido que en la mayoría de ocasiones se materializa con el auxilio de profesionales, expertos y peritos informáticos.

Por tanto, se entra en el plano de una libre valoración siempre guiada por las reglas de la lógica, la argumentación racional, la técnica y el estado de la ciencia.

5.2.2. Excepción a la libre valoración: el documento público electrónico.

El documento público electrónico no está sometido a la libre valoración del juez como criterio rector. Se trata de los documentos como pueda ser el documento nacional de identificación electrónico (DNI), documentos administrativos, de Hacienda, de la Seguridad Social o las escrituras notariales firmadas digitalmente.

Todos estos documentos tienen atribuidos un valor privilegiado como prueba, escapan claramente a la regla valorativa de libre apreciación. Aun así, es necesario remarcar que existe la posibilidad de instar la comprobación de que ha existido manipulación, falsificación o producción de forma fraudulenta, a través de una justificación de peso, o con un principio de prueba con el que se pueda constatar tales hechos.

¹²⁸ García Paredes, Antonio. *La prueba en juicio: ¿y si es electrónica?* Revista de Contratación Electrónica” número 62, julio 2005. Pág. 26.

Los documentos públicos autorizados por notario que se hallan en formato o soporte electrónico, de igual forma que ocurre con los autorizados sobre papel, gozan de fe pública y su contenido se presume veraz e íntegro¹²⁹.

Por lo que se refiere a la llamada “escritura electrónica notarial” ésta implica la existencia de un tercero imparcial, el notario electrónico, que se encuentra legitimado para certificar la identidad del firmante, emitiendo certificaciones del documento cuyo original archiva con la posibilidad de acreditar la fecha y hora de creación del documento o de realización de la copia¹³⁰.

5.2.3. Acceso a la prueba electrónica.

Para poder valorar una prueba electrónica es necesaria que ésta se haya obtenido de forma lícita, accediendo a su contenido por cauces legales. En fase de instrucción es cuando se pueden dar más problemas por las dificultades que entraña el acceso al contenido de la prueba electrónica que se halle en soportes electrónicos. Así, las tareas policiales de investigación pueden topar con claves que protejan los aparatos electrónicos así como sistemas de encriptación que impidan leer o visualizar su contenido.

En estos casos no cabe posibilidad de obligar al titular de la información a que facilite las claves, programas o demás tareas necesarias para acceder al contenido protegido. Ello es porque constitucionalmente se protege el derecho a no declarar y a no contestar a las preguntas que se estimen convenientes para su defensa, pues de otra forma se estaría colaborando indirectamente a su presunta incriminación obligándole a responder.

La válvula de escape para que las tareas de investigación puedan dar frutos y obtener la máxima información posible se encuentra en la utilización de programas que puedan servir para conseguir la contraseña o desenscriptar el texto o imágenes bajo clave sin acudir al titular del mismo.

¹²⁹ Art. 17 bis de la Ley de 28 de mayo 1862, Orgánica del Notariado.

¹³⁰ Bolás Alfonso, Juan. (2000). *Firma electrónica, comercio electrónico y fe pública notarial*. Revista Jurídica del Notariado, oct-dic. Pág. 15-20.

5.2.4. Manipulación.

Los soportes electrónicos son fácilmente manipulables, por ello éste es un punto que el juzgador tiene muy en cuenta a la hora de dotar de valor a la prueba que en aquél soporte electrónico se encuentre. Es un tema conflictivo dado el margen de subjetividad que ofrece y la posible indefensión que puede causar al no aceptarse como prueba por su supuesta manipulación, o al sí aceptarse y tenerse en cuenta habiendo ésta sido manipulada.

A este respecto, la jurisprudencia del Tribunal Supremo¹³¹ se ha pronunciado de la siguiente forma:

- “Las simples y retóricas alegaciones sobre un presunto hecho (sobre el caso de la denuncia de manipulación de prueba electrónica) no tienen entidad suficiente para desacreditar una prueba de cargo.
- Es el recurrente, la persona que alega algo, quien ha de asumir el desafío probatorio de acreditar la existencia de alguna grieta estructural que invalide la eficacia de la prueba en su contra”.

Por otro lado, respecto a las pruebas electrónicas contenidas en documentos, se debe de realizar una distinción entre el documento con firma electrónica y aquellos que no aparecen así signados. Los primeros, con independencia de cómo se hayan elaborado, una vez se ha estampado la firma digital en ellos es imposible la modificación del documento, por tanto, queda constancia de su no manipulación. En cambio, en el resto de documentos informáticos no firmados mediante la garantía que ofrece la firma electrónica, pueden suscitar problemas respecto a su integridad y autoría.

5.2.5. Concurrencia de pruebas.

La prueba electrónica no representa en sí una superioridad probatoria, sino que requiere del complemento o refuerzo de otras pruebas tradicionales, para realizar un ejercicio de valoración global y así acceder a un resultado determinado.

Es por ello necesario y frecuente la denominada concurrencia de pruebas, es decir, un conjunto de medios probatorios a valorar según su clase y cuyo concurso es necesario para ponderar el alcance de la prueba electrónica.

¹³¹ STS núm. 249/2008, de 20 de mayo, F.J. 2º y 3º (RJ 2008\4387).

Así, por ejemplo, cuando dentro de un proceso judicial se presenta como prueba la voz o imágenes grabadas en vídeo y las partes discrepan sobre éstas, el juzgador para poder realizar su tarea de valoración de forma lógica y proporcional debería, en la medida de lo posible y conveniente, llamar y escuchar como testigo a todo aquel que pudiera dar luz sobre dicho material, ya fuere en sentido técnico como en lo relativo a las circunstancias fácticas del cómo, dónde y cuándo se efectuó tal grabación así como el resto de información que pueda aportar¹³².

5.2.6. Pericia informática.

El conocimiento privado del Juez respecto a las nuevas tecnologías no va ser en todos los casos el más alto ni el más idóneo, sino que el órgano juzgador puede desconocer por completo las distintas formas electrónicas y medios informáticos que se van desarrollando en la sociedad. Pese a ello, no es posible que tal desconocimiento impida una tutela judicial efectiva que se haga depender de que el órgano juzgador sepa más o menos sobre las nuevas tecnologías.

En esta línea, algunos autores¹³³ defienden como inexcusables dos puntos: la práctica en todos los casos de la pericia informática y que el lenguaje expositivo y las conclusiones sean de la máxima claridad. De esta forma, se introduce objetividad y transparencia para suplir al desconocimiento, la subjetividad o el oscurantismo.

Solamente disponiendo de todo ese material, de los conocimientos personales suficientes (como son las expresiones técnicas del caso) y de la pericia judicial o informes de las partes, que especifiquen lo sucedido y ofrezcan conclusiones claras y científicamente avaladas, podrá estarse en las condiciones idóneas de efectuar una adecuada valoración de esos concretos medios de prueba electrónicos.

¹³² Mora Díaz, Rocío (2006). La valoración de la prueba en soportes informáticos. Noticias jurídicas, sección artículos doctrinales. Pág. 3-16.

¹³³ Como Urbano Castrillo, Eduardo. (2009). La valoración de la prueba electrónica. Valencia: ed. Tirant Lo Blanch. Pág. 47 y ss.

6. LOS PROBLEMAS QUE REPRESENTA LA INFORMACIÓN DIGITAL.

6.1. Proliferación y fragmentación legal.

El uso de pruebas electrónicas se ha convertido en un elemento necesario para tratar de esclarecer delitos cometidos a través de dispositivos electrónicos, así como otro tipo de delitos en los que la información contenida en un soporte electrónico es clave para que el órgano juzgador pueda emitir su decisión.

Tal y como se ha expuesto a lo largo del presente trabajo, los dos problemas más importantes entorno a la temática de la prueba digital son: por un lado, el constante crecimiento y desarrollo de la tecnología y, por otro lado, la escasa legislación al respecto.

El primero de estos problemas, es el revolucionario proceso de penetración de la informática, la tecnología y los datos digitales en la vida cotidiana de la población. Esta evolución ha ido generando múltiples dudas en torno a su uso, tanto para perpetrar delitos como para ser utilizados como elementos de prueba.

Los órganos enjuiciadores no tienen obligación alguna de ser expertos en todas las materias tecnológicas, así como tampoco las partes conocen los entresijos del mundo digital, haciendo que las pruebas electrónicas sean un arma de doble filo. Si bien es cierto que en los tribunales se cuenta con el soporte de profesionales, expertos, técnicos y peritos para solventar el referido desconocimiento, no es menos cierto que la tecnología día a día va cambiando produciendo gran incertidumbre respecto a su utilización.

Respecto al segundo problema, la carente normativa jurídica en nuestro país en relación a las pruebas electrónicas no debe suponer un obstáculo para el uso de las tecnologías emergentes, tanto a nivel personal, doméstico, como a nivel empresarial. De igual forma la no regulación específica de todos los parámetros, criterios de admisión y valoración, no puede suponer un obstáculo que impida el derecho a la defensa de las partes en un proceso, que implique inseguridad jurídica, impidiendo utilizar como medio de prueba válido las nuevas tecnologías.

Existe una dificultad en el establecimiento del valor jurídico de este tipo de pruebas debido al desconocimiento sobre los procedimientos de procesado de datos y de la

interpretación de las leyes procesales al respecto. También existen dificultades para su preservación y una escasa información sobre cómo almacenarla correctamente para su conservación. Esta barrera viene generada por la falta de una regulación propia y sistemática, así como por la falta de jurisprudencia homogénea.

Nuestro ordenamiento jurídico no cuenta con un procedimiento específico que regule la obtención, conservación y presentación de la prueba electrónica ante los Tribunales de Justicia, por lo que se aplica por analogía la regulación del procedimiento general de la prueba tradicional. Pese que ésta pueda parecer una solución razonable, la casuística no indica lo mismo, pues las pruebas electrónicas tienen unas particularidades que hacen que se generen dudas y que no se puedan subsanar con la simple aplicación analógica de la prueba en general ni el recurso a la jurisprudencia.

6.2. Los problemas procesales vinculados a la cadena de custodia.

Otro de los grandes problemas que envuelven a la prueba electrónica es el relativo a su fiabilidad.

Aunque puede considerarse que su objetividad y exactitud la hace más fiable y por lo tanto, más conveniente y provechosa su utilización, no es menos cierto que la falta de conocimientos para verificar su autenticidad hace que sea considerada más vulnerable y, por lo tanto, menos fiable que una prueba tradicional, constituyendo un inconveniente para su uso y admisibilidad.

La forma de garantizar la autenticidad e integridad de la fuente probatoria es mantener la cadena de custodia de los elementos electrónicos incautados¹³⁴.

El elemento más importante es el orden: es necesario mantener una cadena de custodia ordenada para que desde el momento en que se intervienen por los cuerpos de seguridad el material, aparatos, equipos y demás soportes electrónicos que contengan las pruebas, hasta el momento en el que éstos sean entregados, según convenga al perito correspondiente o al Secretario Judicial, no exista posibilidad de entregar algo diferente a lo ocupado o intervenido, es decir, no exista manipulación¹³⁵.

¹³⁴ Abel Lluch, Xavier. (2012). Derecho probatorio...Ob.Cit. Pág. 984.

¹³⁵ La SAN núm. 30/2009, de 30 abril, F.J. 3º (JUR 2010\80227), es un ejemplo de caso en el que se comprueba que lo incautado no corresponde con lo recibido y analizado por el Juzgado.

El Tribunal Supremo se ha manifestado en varias ocasiones sobre el problema de la cadena de custodia, expresando que el objetivo final es el de garantizar que desde el momento en que se recogen los vestigios hasta que llegan a concretarse como pruebas electrónicas en el momento del juicio, aquello sobre lo que recaerá la inmediación, publicidad y contradicción de las partes así como la valoración judicial, debe ser lo mismo. Es imprescindible tener la certeza y seguridad de que lo que se ha trasladado y analizado no cambia, es lo mismo en todo momento¹³⁶.

A este respecto, encontramos jurisprudencia más concreta¹³⁷ que, interpretando el artículo 338 de la LECrim, establece la necesidad de cumplir los siguientes requisitos:

- Debe realizarse una descripción del material ocupado en Acta o Diligencia del Secretario Judicial y en presencia del mismo debe realizarse el bloqueo y precinto de cualquier ranura, puerto o disquete existente en el soporte electrónico incautado.
- Las pruebas electrónicas deberán ser custodiadas en lugar adecuado, evitando el acceso a personas ajenas, su deterioro así como su manipulación.
- En la causa deberá dejarse constancia de la cadena de custodia llevada a cabo, en caso que transcurra un tiempo entre la ocupación y la entrega al Secretario Judicial.
- Deberá existir un control judicial respecto a la recogida y su custodia, pues de no existir éste, afectaría a la validez de la prueba, vulnerándose el derecho a un proceso con todas las garantías.

Es necesario apuntar que en caso de que existiera una irregularidad en la cadena de custodia llevada a cabo, ello no constituiría una vulneración de derecho fundamental alguno, puesto que sólo sería así de admitir y dar valor a una prueba que hubiera sido conseguida sin respetar las garantías jurídicas esenciales del procedimiento, en especial el derecho a la defensa. La jurisprudencia ha entendido que el sólo apunte de la

¹³⁶ Las sentencias en las que se basa esta afirmación son la STS núm. 6/2010, de 27 enero. (RJ 2010\3008) y STS núm. 776/2011, de 20 julio (RJ 2012\3380).

¹³⁷ Como recuerda la STC núm. 174/2003, de 29 septiembre (RTC 2003\174).

posibilidad de manipulación de la cadena de custodia no es suficiente para desvirtuar la prueba, pues es necesario que se consiga probar su manipulación efectiva¹³⁸.

6.3. Especial relevancia en el orden penal: los delitos informáticos.

Si bien a lo largo del presente trabajo se ha estudiado cómo las pruebas electrónicas pueden ser utilizadas dentro de un proceso penal para poder sustentar una acusación o defensa, también es necesario apuntar a la cada vez mayor utilización de soportes electrónicos para perpetrar delitos a través de los mismos.

Aunque el Código Penal español no contempla de forma expresa una subespecie de “delitos informáticos”, diversas voces proponen la necesidad de diferenciarlos del resto de delitos tradicionales, por la distinta perspectiva y matices que ofrecen. Pese a ello, es necesario recordar que los delitos informáticos son los mismos que los tradicionales pero perpetrados a través de otros medios.

6.3.1. Delitos informáticos a nivel europeo.

En noviembre de 2001 se firmó en Budapest el “Convenio de Ciberdelincuencia del Consejo de Europa”, con la finalidad de dibujar un marco de referencia en el campo de las tecnologías y los delitos en la Unión Europea.

En el referido convenio se define los delitos informáticos como “actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos”.

Además, en el mismo, se establece una propuesta de clasificación para agrupar los tipos de delitos informáticos en cuatro bloques:

A. Delitos informáticos:

- Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.
- Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

¹³⁸ STS núm. 629/2011, de 23 junio ,F.J. 3º (RJ 2012\10535) y STS núm. 776/2001 de 20 julio F.J. 2º y 3º (RJ 2001\6865).

B. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

- Acceso ilícito a sistemas informáticos.
- Interceptación ilícita de datos informáticos.
- Interferencia en el funcionamiento de un sistema informático.
- Abuso de dispositivos que faciliten la comisión de delitos.

C. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines:

- Un ejemplo de este grupo de delitos es la copia y distribución de programas informáticos, o piratería informática.

D. Delitos relacionados con el contenido:

- Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

De forma más reciente, en enero de 2008 se promulgó el “Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa” que incluye, entre otros aspectos, las medidas que se deben tomar en casos de difusión de material xenófobo o racista, de insultos o amenazas con motivación racista o xenófoba y de negociación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.

6.3.2. Delitos informáticos en España.

Siguiendo la legislación española, el art. 299 LECrim y de forma concreta, la sistemática del vigente Código Penal español, existen tres categorías fundamentales donde se pueden englobar los ilícitos penales considerados como delitos informáticos. Son los siguientes:

A. Delitos económico patrimoniales vinculados a la informática:

Se trata de la denominada ciberdelincuencia económica, es decir, ataques contra el patrimonio ajeno como bien jurídico, teniendo como finalidad última la de apoderarse o beneficiarse económicamente del patrimonio de terceras personas. La especialidad de éstos es que se realiza a través de la informática. Siguiendo el CP podemos destacar:

- El robo inutilizando sistemas de guardia criptográfica (art. 238.5 CP).
- La estafa informática, ya sea por ingeniería social o por ingeniería informática. La primera de ellas es a través de engaño a personas y la segunda se perpetra a través de manipulación informática o actuaciones semejantes (art 248.2 CP)¹³⁹.
- Defraudación de telecomunicaciones informáticas (art. 255 CP).
- Hurto de tiempo informático, o uso no autorizado de terminales informáticas (art. 256 CP).
- Virus o daños informáticos sobre datos (art. 346 y 571 CP).
- Contra la propiedad intelectual informática, en cualquiera de sus modalidades reguladas (art. 270.3 CP), contra la propiedad industrial, también en cualquiera de sus modalidades (art273-275 CP).
- Espionaje informático de secretos de empresa (art. 278-280 CP)¹⁴⁰.
- Los delitos relativos a la publicidad engañosa (art. 282 CP), a la manipulación en aparatos en perjuicio del consumidor (art. 283 CP) o contra el mercado informático (art. 286 CP).
- Blanqueo informático de capitales (art. 301 CP).
- Falsedad documental, en aquellos casos en los que el soporte sea de naturaleza informática (art. 390 en relación con el art. 26 CP).

B. Atentados por medios informáticos contra la intimidad y la privacidad

Se trata de la llamada ciberdelincuencia intrusiva, es decir, el ataque a la privacidad y a la intimidad como bienes jurídicos protegidos en el art. 18 CE, abarcando el derecho al honor, la intimidad personal, familiar, la propia imagen, el domicilio, el secreto de las

¹³⁹ Un ejemplo de delito económico patrimonial vinculado a la informática, considerado como estafa informática lo encontramos en la STS núm. 860/2008 de 17 diciembre (RJ 2009\131).

¹⁴⁰ Un caso calificado como espionaje informático, dentro del delito económico patrimonial vinculado a la informática es el de la STS núm. 97/2003 ,de 2 junio (RTC 2003\97).

comunicaciones y el uso correcto de la informática. Los tipos penales recogidos a este respecto en el CP son los siguientes:

- Amenazas y coacciones a través de medios informáticos (art. 169 y 172 CP).
- Distribución de material pornográfico y pornografía infantil (art. 186 a 189 CP)¹⁴¹.
- Descubrimiento y revelación de secretos gracias a medios informáticos (art. 197 a 200 CP).
- Injurias y calumnias informáticas (art. 205 a 216 CP).
- Cesión no consentida de datos ajenos, a través de la infidelidad en la custodia de documentos y violación de secretos para su venta, hecha por funcionario el cual la tiene prohibida (art. 417, 418 y 423 CP).

C. Ataques por medios informáticos contra intereses supraindividuales

Se trata del ciberespionaje y ciberterrorismo, es decir, ataques considerados más graves, que afectan de forma indiscriminada a los intereses generales de los ciudadanos, con la intención de crear miedo e incertidumbre, para subvertir el sistema político o de conveniencia que reine. En la ley penal española encontramos los siguientes tipos:

- Usurpación de funciones públicas mediante correo electrónico (art. 402 CP).
- Descubrimiento y revelación de secretos relativos a la Defensa nacional (art. 598 y 603 CP).

¹⁴¹ Un ejemplo de atentado contra la intimidad y la privacidad a través de medios informáticos, calificado como distribución de material pornográfico es la STS núm. 739/2008, de 12 noviembre, (RJ 2009\167).

7. CONCLUSIONES

Actualmente nos encontramos en una sociedad en la que los soportes electrónicos suponen una herramienta esencial en todos los ámbitos de la vida. En el ámbito jurídico los mismos pueden ser de gran utilidad, aunque su uso no se encuentre exento de dificultades.

Debido a que los avances informáticos resultan imparables, la sociedad no puede estancarse, sino que la observación, el aprendizaje y la adaptación al medio electrónico deben ser los ingredientes para el éxito en la utilización de los nuevos sistemas tecnológicos.

Los medios electrónicos ofrecen grandes ventajas y es por ello que resulta muy beneficioso conocer los secretos de la nueva era digital y las formas de aprovechar al máximo los recursos que nos puede aportar.

1. Las ventajas de la prueba electrónica. Entre las múltiples ventajas que ofrece la prueba electrónica encontramos que ésta proporciona una información exacta, completa, clara, precisa, rigurosa, veraz y objetiva.

Ello es porque la fuente de la que emana la prueba electrónica no contiene subjetividad alguna, a diferencia de lo que ocurre con otro tipo de pruebas como puede ser la testifical, la cual está cargada de subjetividad por el componente humano.

2. Las desventajas de la prueba electrónica. Al lado de la utilidad y de las ventajas que ofrecen los nuevos medios tecnológicos, nos encontramos con el riesgo y la inseguridad que supone su sencilla manipulación y aprovechamiento para realizar conductas maliciosas, tales como crear coartadas ficticias, eliminar pruebas reales, incriminar a terceros no intervinientes, etc.

3. La formación judicial específica. En los últimos años han aparecido una gran cantidad de nuevos medios probatorios, además de los que están por descubrir y por tanto, inexistentes en estos momentos, al depender de los avances de la ciencia.

Ello origina una problemática constitutiva de la nueva frontera de la prueba, que obliga tanto a jueces, magistrados como a los cuerpos de seguridad a intentar que las técnicas de investigación sean escrupulosas, con el objeto de garantizar que el material incautado

no sufra alteraciones o deje de tener validez por errores legales en su obtención y custodia, así como también quedan obligados a adaptarse y estar permanentemente alerta a la más reciente jurisprudencia nacional y extranjera, para conocer el tratamiento jurídico que se da a las últimas innovaciones.

4. La complejidad de la prueba electrónica. Las fuentes electrónicas cuentan con una gran diversidad, con una constante innovación debido a su continuo desarrollo y con una alta complejidad para captar su funcionamiento, derivado del componente técnico-científico que llevan aparejadas.

Ello comporta la necesidad de contar con la pericia informática, que resulta indispensable en la mayoría de los casos de cierta dificultad o controversia. Se deposita la confianza en la formación, conocimiento y experiencia de los expertos respecto a la obtención, análisis y conservación de la prueba electrónica.

5. La fiabilidad de la prueba electrónica. La perfección de la tecnología va unida a las inmensas posibilidades de que ésta se utilice para manipular la realidad que trata de presentar. De ahí nace la necesidad de comprobar que no existe deformación, adulteración ni falsificación en las pruebas electrónicas debiendo éstas pasar el test de admisibilidad que confirme su integridad, autenticidad y licitud.

6. Acceso de la prueba electrónica al proceso. Debido a la gran diversidad de soportes electrónicos existentes, son múltiples las formas de acceder a su contenido. En todo caso, el acceso a lo encerrado en la prueba electrónica será posible: porque haya sido aportada por alguna de las partes, porque se haya aprehendido fuera o dentro de lugar cerrado o como consecuencia de la realización de un registro de información accesible.

Los cauces por los que se puede incorporar la prueba electrónica en el proceso penal pueden ser: a través de la prueba pericial, cuando se precisen conocimientos técnico-científicos, como reconocimiento judicial en los casos que sea necesario que el Juez perciba directamente la prueba, como prueba documental, para aquellos supuestos en los que sea posible presentar el contenido probatorio en documento, a través de la reproducción de palabras sonidos e imágenes cuando se quiera reproducir lo contenido en instrumentos de filmación, grabación u otros semejantes, o gracias a la prueba testifical que puede ayudar al órgano juzgador a formar su convicción.

7. *Eficacia probatoria.* La prueba electrónica tiene la misma validez procesal que las pruebas que se actúan de manera convencional o tradicional. Puesto que por el avance de la tecnología hay hechos jurídicos que pueden captarse por medios electrónicos, éstos si se incorporan en la forma correcta, en el momento procesal oportuno y respetan la integridad, autenticidad y licitud que la jurisprudencia exige, darán certeza a los juzgados sobre los hechos acontecidos.

8. *La insuficiente regulación de la prueba electrónica.* Los problemas jurídicos que se originan por la escasa legislación española respecto a este tipo de prueba, obligan a atender de un lado, a las reglas analógicas que proporcionan otras instituciones mejor reguladas o con un cuerpo de jurisprudencia ya existente y, de otro, estudiar la legislación comparada a fin de extraer criterios útiles para ponderar y valorar las dificultades interpretativas que presentan.

Si bien en los últimos años se ha experimentado una considerable aparición de regulación específica en lo relativo a los medios electrónicos, la normativa vigente es fuente importante de problemas de interpretación y aplicación, destacándose entre ellos el de la naturaleza que se atribuye a los instrumentos regulados o el de la razón de ser del criterio de valoración escogido.

Aún no se ha regulado de forma específica cómo han de ser tratadas a nivel procesal las pruebas electrónicas, quedando su fuerza probatoria sometida a la voluntad del juzgador. Por tanto, siguen siendo inciertos los parámetros que han de regir la prueba electrónica dentro del proceso, reduciéndose de esta forma su utilidad y quedando ésta desvirtuada por la inseguridad jurídica existente.

8. BIBLIOGRAFIA

1. Abel Lluch, Xavier (dir); Ginés Castellet, Núria (coor.). (2006). *Empresa y prueba informática*. Barcelona: ed. Bosch Editor.
2. Abel Lluch, Xavier. (2012). *Derecho probatorio*. Madrid: ed. Bosch Procesal.
3. Abel Lluch, Xavier; Picó i Junoy, Joan; Richard González, Manuel (dir). (2011). *La prueba judicial. Desafíos en las jurisdicciones civil, penal, laboral y contencioso-administrativa*. Madrid, Ed. La Ley.
4. Abel Lluch, Xavier; Picó Junoy, Joan. (dir). (2008). *Colección de Formación Continua de la Facultad de Derecho de ESADE*. Serie Estudios Prácticos sobre los medios de prueba, núm. 2. Barcelona: ed. J. M. Bosch.
5. Barrios González, Boris. (2004). *Ideología de la prueba penal*. (2ª edición). Ed. Jurídica Ancon.
6. Bolás Alfonso, Juan. (2000). *Firma electrónica, comercio electrónico y fe pública notarial*. Revista Jurídica del Notariado, oct-dic.
7. Bonachera Villegas. (2012). *El registro de archivos informáticos: una cuestión necesitada de regulación*. En Revista General de Derecho Procesal 27.
8. Cabañas García, Juan Carlos. (1993). *La valoración de las pruebas y su control en el proceso civil*. Madrid: ed. Trivium.
9. Cabezudo Rodríguez, N. (2004). *Omisiones del legislador procesal ante los medios de prueba tecnológicos*. Madrid: ed. La Ley.
10. Calderón Cuadrado, Mª Pía sobre la sociedad de la información y modernización de la justicia, en su obra (2011). *La encrucijada de una justicia penal tecnológicamente avanzada*. Madrid: ed. La Ley.
11. Castillejo Manzanares, Raquel. (2010) *Medios Probatorios. Hacia un nuevo proceso penal. Cambios necesarios*". Madrid: ed. La Ley.
12. Castillejo Manzanares, Raquel. (2010). En "Medios Probatorios", dentro del libro "Hacia un nuevo proceso penal. Cambios necesarios". Madrid: ed. La Ley.
13. De Diego Díez, Luis Alfredo. (2005). *Ocupación, conservación y destrucción de las piezas de convicción*. Valencia: Ed. Tirant lo Blanch.
14. De Diego Díez, Luis Alfredo. *Control judicial sobre las piezas de convicción: la puesta a disposición judicial*. Diario la Ley, núm. 6196, Sección Doctrina, 23 de febrero de 2005.

15. Díaz Cabiale, José Antonio. (1992). *La admisión y práctica de la prueba en el proceso penal*. Madrid: editado por el CGPJ.
16. Ferrer Beltrán, Jordi. (2007). *La valoración racional de la prueba*. Madrid: ed. Marcial Pons.
17. García Paredes, Antonio. *La prueba en juicio: ¿y si es electrónica?*. Revista de Contratación Electrónica” número 62, julio 2005.
18. Gómez del Castillo y Gómez, Manuel. (2009). *Aproximación a los nuevos medios de prueba en el proceso civil*. Revista "Derecho y conocimiento" de la Facultad de derecho de la Universidad de Huelva.
19. López Simó, Francisco. (2001). *Disposiciones generales sobre la prueba*. Madrid: ed. La Ley.
20. Martí Mingarro, Luis. (2003). *La prueba ilícita penal*. (3ª edición). Navarra: ed. Aranzadi SA.
21. Martín García, Pedro. (2000). *La prueba en el proceso penal*. Valencia: ed. Revista General de Derecho.
22. Montero Aroca, Juan; Gómez Colomer José Luis; Montón Redondo, Alberto; Barona Vilar, Silvia. (2013). *Derecho Jurisdiccional III, proceso penal*. (21ª edición). Valencia, Ed. Tirant lo Blanch.
23. Montero Aroca, Juan; Gómez Colomer José Luis; Montón Redondo, Alberto; Barona Vilar, Silvia. (2013). *Derecho Jurisdiccional III, proceso penal*. (21ª edición). Valencia: Ed. Tirant lo Blanch.
24. Mora Díaz, Rocío (2006). *La valoración de la prueba en soportes informáticos*. Noticias jurídicas, sección artículos doctrinales.
25. Muñoz Sabaté, Lluís. (2007). *Introducción a la probática*. Colección de Formación Continua Facultad de Derecho ESADE. Barcelona: ed. Bosch Formación.
26. Muñoz Sabaté, Lluís. (2009). *Curso de probática judicial*. Madrid: ed. La Ley.
27. Ortiz Pradillo, Juan Carlos (2008). *Nuevas medidas tecnológicas de investigación criminal para la obtención de la prueba electrónica*. Madrid: ed. La Ley.
28. Pasamar, A. (2006). *Empresa y prueba informática en el libro del mismo título “Empresa y Prueba informática”*. Colección de formación continua de la Facultad de Derecho ESADE. Barcelona: ed. URL, J.M. Bosch.

29. Rivera Morales, Rodrigo. (2011). *La prueba: un análisis racional y práctico*. Madrid: ed. Marcial Pons.
30. Sánchez Núñez, Teresa. (2007). *Jurisprudencia del Tribunal Constitucional sobre el uso de las nuevas tecnologías en la investigación penal*. Cuadernos de Derecho Judicial. Madrid: editado por el Consejo General del Poder Judicial.
31. Sanchís Crespo, Carolina. (1999). *La prueba por soportes informáticos*. Valencia: ed. Tirant lo Blanch.
32. Taruffo, Michele. (2010). *Simply la verdad: el juez y la construcción de los hechos*. Madrid: ed. Marcial Pons.
33. Taruffo, Michelle. (2008). *La prueba*. Madrid: ed. Marcial Pons.
34. Urbano Castrillo, Eduardo. (2009). *La valoración de la prueba electrónica*. Valencia: ed. Tirant Lo Blanch.
35. Vegas Torres, Jaime. (1996). *Prueba ilícita en particular (II): la ilicitud de la entrada y registro en lugar cerrado y sus consecuencias*. Cuadernos de Derecho Judicial. Madrid: editado por el Consejo General del Poder Judicial y la Escuela Judicial.
36. Younes Jerez, Simón. (2001). *Credibilidad y certeza en la prueba judicial*. Madrid: Ed. Leyer.

9. ANEXO DE JURISPRUDENCIA

Tribunal Constitucional:

1. STC núm. 115/2013, de 9 de mayo, F.J. 3º (RTC 2013\115).
2. STC núm. 173/2011 de 7 noviembre, F.J. 4º (RTC 2011\173).
3. STC núm. 480/2009, de 22 mayo, F.J. 1º y 2º (RJ 2010\662).
4. STC núm. 208/2007, de 24 de septiembre, (RTC 2007\208).
5. STC núm. 1305/2006, de 27 diciembre (RJ 2007\501).
6. STC núm. 1/2004 de 14 de enero, F.J. 2º (RTC 2004\1).
7. STC núm. 174/2003, de 29 septiembre (RTC 2003\174).
8. STC núm. 71/2003 de 9 abril, F.J. 3º (RTC 2003\71).
9. STC núm. 183/2002, de 14 octubre, F.J. 2º (RTC 2002\183).
10. STC núm. 168/2002, de 30 septiembre, F.J. 3º (RTC 2002\168).
11. STC núm. 202/2001, de 15 octubre F.J.3º (RTC 2001\202).
12. STC núm. 37/2000, de 14 de febrero, F.J. 3º (RTC 2000\37).
13. STC núm. 210/1999, de 29 noviembre, F.J. 2º (RTC 1999\210).
14. STC núm. 161/1999, de 27 septiembre, (RTC 1999\161).
15. STC núm. 88/1999 de 26 mayo, F.J. 2º y 3º (RTC 1999\88).
16. STC núm. 325/1994, de 12 de diciembre, F.J. 2º (RTC 1994\325).
17. STC núm. 190/1992, de 16 noviembre, F.J. 2º (RTC 1992\190).
18. STC núm. 68/1991, de 8 abril, F.J. 2º (RTC 1991\68).
19. STC núm. 128/1990 de 5 julio (RTC 1990\128).
20. STC núm. 264/1988, de 22 diciembre. F.J. 2º y 3º (RTC 1988\264).
21. STC núm. 51/1985, de 10 de abril de 1985, F.J.2º (RTC 1985\51).

Tribunal Supremo

1. STS núm. 776/2011, de 20 julio F.J. 2º (RJ 2012\3380).
2. STS núm. 629/2011, de 23 junio, F.J. 3º (RJ 2012\10535)
3. STS núm. 492/2010, de 18 mayo, F.J. 1º (RJ 2010\5814)
4. STS núm. 6/2010, de 27 enero (RJ 2010\3008).
5. STS núm. 1295/2009, de 9 diciembre, F.J. 3º (RJ 2010\303).
6. STS, de 4 de noviembre de 2009, F.J. 2º (La Ley 226669/2009).

7. STS núm. 860/2008 de 17 diciembre (RJ 2009\131).
8. STS núm. 785/2008, de 25 noviembre, F.J. 2º (RJ 2009\556).
9. STS núm. 739/2008, de 12 noviembre, (RJ 2009\167).
10. STS núm. 249/2008, de 20 de mayo, F.J. 2º y 3º (RJ 2008\4387).
11. STS, de 9 de mayo de 2008, FJ 2º y 3º (RJ 2008/4648).
12. STS núm. 90/2007, de 23 enero, F.J. 3º (RJ 2007\625).
13. STS núm. 855/2006, de 12 septiembre, F.J. 2º (RJ 2006\6345).
14. STS núm. 285/2006, de 8 marzo, F.J. 2º (RJ 2006\1003).
15. STS núm. 341/2005, de 17 de marzo, (RJ 2005\3561).
16. STS núm. 992/2003, de 3 julio, (RJ 2003\6153).
17. STS núm. 97/2003, de 2 junio (RTC 2003\97).
18. STS núm. 669/2003, de 7 mayo, F.J. 4º (RJ 2003\5258).
19. STS núm. 1464/2002 de 13 septiembre, F.J. 2º. (RJ 2002\8443).
20. STS núm. 776/2001 de 20 julio F.J. 2º y 3º (RJ 2001\6865).
21. STS, de 2 de diciembre de 2000, F.J. 2º (RJ 2000/9955).
22. STS núm. 1311/2000, de 21 julio, (RJ 2000\6917).
23. STS núm. 346/1999, de 3 marzo, F.J. 1º t 2º (RJ 1999\2091).
24. STS núm. 1234/1998, de 22 octubre, F.J. 2º (RJ 1998\8716).
25. STS núm. 497/1998, de 3 abril, F.J. 3º (RJ 1998\3284).
26. STS núm. 1611/1997, de 29 de diciembre, (RJ 1997\9098).
27. STS núm. 651/1996, de 4 de octubre (RJ 1997\816).
28. STS núm. 1067/1992, de 30 noviembre, F.J.1º. (RJ 1992\9458).
29. STS de 2 de marzo de 1992 (RJ 1992, 1677).
30. STS, de 19 de abril de 1991, F.J. 4º (RJ 1991/2813).
31. STS, de 3 de julio de 1989 (RJ 1989/5283).
32. STS, de 12 de diciembre de 1988, (RJ/9435).
33. STS de 18 abril de 1988, F.J. 2º y 3º (RJ 1988\2801).
34. STS, de 6 de marzo de 1987 F.J. 2º (RJ 1987\2454).
35. STS, de 30 de noviembre de 1981, F.J. 2º (RJ 1981/4680).

Audiencia Nacional

1. SAN 31/2009, de 30 abril (JUR 2009\244859).

Audiencia Provincial

2. SAP de Cádiz, núm. 31/2014, de 28 enero, F.J. 1º y 2º (JUR 2014\95996).
3. SAP de Pontevedra, núm. 10/2014, de 10 enero, F.J. 2º y 3º (JUR 2014\25448).
4. SAP de Tarragona núm. 220/2013, de 29 mayo, F.J. 1º (JUR 2013\272852).
5. SAP de Madrid, núm. 12/2013, de 5 abril, F.J. 2º (JUR 2013\175198).
6. SAP de Madrid, núm. 1260/2012, de 1 octubre, F.J. 2º (JUR 2012\341849).
7. SAP de Madrid núm. 362/2011, de 25 abril, F.J. 1º y 2º (JUR 2011\249542).
8. SAP de Madrid núm. 46/2011, de 10 febrero, F.J. 2º (JUR 2011\161073).
9. SAP de Barcelona núm. 95/2008, de 29 enero, (ARP 2008\317).
10. SAP de Córdoba núm. 136/2002, de 25 mayo, F.J. 2º (AC 2002\1000)
11. SAP de Valencia núm. 127/2001, de 24 mayo, F.J. 3º (ARP 2001\589).
12. SAP de Madrid, de 23 noviembre 2000, F.J. 2º (AC 2002\136).
13. SAP de Valencia núm. 30/1999, de 1 de febrero, F.J. 1º y 2º (ARP 1999\921).
14. SAP de Tarragona núm. 457/1998, de 1 septiembre, (ARP 1998\3818).